SOC21537 US
#2

jc531 U.S. PTO
09/741668
12/19/00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されてる事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed this Office.

出願年月日
Date of Application: １９９９年１２月２０日

出願番号
Application Number: 平成１１年特許願第３６１２２５号

出願人
Applicant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１０月１３日

特許庁長官
Commissioner,
Patent Office 及川耕造

【書類名】　特許願
【整理番号】　9900698611
【提出日】　平成11年12月20日
【あて先】　特許庁長官殿
【国際特許分類】　H09L 12/16
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　野中　聡
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　江崎　正
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
　【代表者】　出井　伸之
【代理人】
　【識別番号】　100094053
　【弁理士】
　【氏名又は名称】　佐藤　隆久
【手数料の表示】
　【予納台帳番号】　014890
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9707389

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　データ処理装置、データ処理機器およびその方法

【特許請求の範囲】

【請求項１】

コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置において、

第１のバスと、

前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第１のバスに接続された演算処理回路と、

前記第１のバスに接続された記憶回路と、

第２のバスと、

前記第１のバスと前記第２のバスとの間に介在するインターフェイス回路と、

前記第２のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、

前記第２のバスに接続された外部バスインターフェイス回路と

を耐タンパ性の回路モジュール内に有するデータ処理装置。

【請求項２】

前記インターフェイス回路を第１のインターフェイス回路とした場合に、前記第１のバスは、前記演算処理回路および前記記憶回路に接続された第３のバスと、前記第１のインターフェイス回路に接続された第４のバスとを有し、

前記データ処理装置は、

前記第３のバスと前記第４のバスとの間に介在する第２のインターフェイス回路

を前記耐タンパ性の回路モジュール内にさらに有する請求項１に記載のデータ処理装置。

【請求項３】

第５のバスと、

記録媒体またはＩＣカードに搭載された認証機能を持つデータ処理回路との間

の通信処理を行い、前記第５のバスに接続された第３のインターフェイス回路と

、

前記第４のバスと前記第５のバスとの間に介在する第４のインターフェイス回路と

を前記耐タンパ性の回路モジュール内にさらに有する請求項２に記載のデータ処理装置。

【請求項４】

前記暗号処理回路は、

公開鍵暗号回路と、

共通鍵暗号回路と

を有する請求項１に記載のデータ処理装置。

【請求項５】

前記記憶回路は、当該データ処理装置の秘密鍵データおよび他の装置の公開鍵データを記憶し、

前記公開鍵暗号回路は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する前記公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成し、

前記共通鍵暗号回路は、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する

請求項４に記載のデータ処理装置。

【請求項６】

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路

を前記耐タンパ性の回路モジュール内にさらに有し、

前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う

請求項５に記載のデータ処理装置。

【請求項７】

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成し、前記第２のバスに接続された乱数生成回路

を前記耐タンパ性の回路モジュール内にさらに有する

請求項１に記載のデータ処理装置。

【請求項８】

前記外部バスインターフェイス回路は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つのデータを記憶する外付けの外部記憶回路と接続される

請求項１に記載のデータ処理装置。

【請求項９】

前記記憶回路に対してのアクセスと、前記外部バスインターフェイスを介した前記外部記憶回路に対してのアクセスとの制御を、前記演算処理回路からの命令に応じて行う記憶回路制御回路と

をさらに有する請求項８に記載のデータ処理装置。

【請求項１０】

前記外部バスインターフェイス回路は、当該データ処理装置が搭載された機器の制御を統括的に行うホスト演算処理装置に接続される

請求項１に記載のデータ処理装置。

【請求項１１】

前記記憶回路および前記外部記憶回路のアドレス空間を管理する記憶管理回路

をさらに有する請求項８に記載のデータ処理装置。

【請求項１２】

前記演算処理回路は、前記権利書データが示す取り扱いに基づいて、前記コン

テンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する

請求項１に記載のデータ処理装置。

【請求項１３】

前記演算処理回路は、前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成し、前記利用制御データに基づいて、前記コンテンツデータの利用を制御する

請求項１２に記載のデータ処理装置。

【請求項１４】

前記共通鍵暗号回路は、前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データとを用いて暗号化する

請求項４に記載のデータ処理装置。

【請求項１５】

有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、

前記記憶回路は、前記ライセンス鍵データを記憶し、

前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し、

前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、

前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する

請求項４に記載のデータ処理装置。

【請求項１６】

前記記憶回路は、ブロック単位でデータの書き込みおよび消去が行われ、

前記演算処理回路によって制御され、前記記憶回路に対してのデータの書き込みおよび消去の許否を前記ブロック単位で管理する書き込みロック制御回路

を前記耐タンパ性の回路モジュール内にさらに有する請求項１に記載のデータ

処理装置。

【請求項１７】

コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置において、

第１のバスと、

前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第１のバスに接続された演算処理回路と、

前記第１のバスに接続された記憶回路と、

第２のバスと、

前記第１のバスと前記第２のバスとの間に介在するインターフェイス回路と、

前記第２のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、

前記第２のバスに接続された外部バスインターフェイス回路と

を耐タンパ性の回路モジュール内に有し、

前記演算処理回路は、前記外部バスインターフェイス回路を介して外部回路から割り込みを受けると、当該外部回路のスレーブとなって当該割り込みによって指定された処理を行い、当該処理の結果を前記外部装置に通知する

データ処理装置。

【請求項１８】

前記演算処理回路は、前記処理の結果を前記外部回路に割り込みを出して通知する

請求項１７記載のデータ処理装置。

【請求項１９】

前記外部バスインターフェイスは、前記演算処理回路および前記外部回路との共有メモリを有し、

前記演算処理回路は、当該共有メモリに前記処理の結果を書き込み、当該処理の結果は前記外部回路からのポーリングによって当該外部回路に通知される

請求項１７に記載のデータ処理装置。

【請求項２０】

前記外部バスインターフェイスは、

前記外部回路から依頼された処理の前記演算処理回路における実行状態を示し、前記演算処理回路によって設定され、前記外部回路によって読まれるフラグを持つ第１のステータスレジスタと、

前記外部回路が前記演算処理回路に処理を依頼したか否かを示し、前記外部回路によって設定され、前記演算処理回路によって読まれるフラグを持つ第２のステータスレジスタと、

前記処理の結果が書き込まれる記憶回路と

を有する請求項１９に記載のデータ処理装置。

【請求項２１】

前記記憶回路は、前記割り込みによって指定される処理を記述した割り込みプログラムを記憶し、

前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行して前記処理を行う

請求項１８に記載のデータ処理装置。

【請求項２２】

前記記憶回路は、複数の前記割り込みプログラムと、当該割り込みプログラムを実行する際に読み出される複数のサブルーチンとを記憶し、

前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行する際に、前記記憶回路から必要に応じて前記サブルーチンを読み出して実行する

請求項２１に記載のデータ処理装置。

【請求項２３】

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置と

を有するデータ処理機器において、

前記データ処理装置は、

権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、

前記決定の結果を示す履歴データを生成する履歴データ生成手段と、

前記コンテンツ鍵データを復号する復号手段と

を耐タンパ性の回路モジュール内に有する

データ処理機器。

【請求項２４】

前記演算処理装置は、前記割り込みタイプを示す割り込みを受けると、当該割り込みタイプに対応した割り込みルーチンを実行して割り込みを前記データ処理装置に出し、

前記データ処理装置は、前記演算処理装置から受けた前記割り込みによって指定された処理に対応する割り込みルーチンを実行する

請求項２３に記載のデータ処理機器。

【請求項２５】

前記データ処理装置は、前記処理の結果を前記演算処理装置に割り込みを出して通知する

請求項２３に記載のデータ処理機器。

【請求項２６】

前記データ処理装置は、当該データ処理装置および前記演算処理装置がアクセス可能な共有メモリを有し、

前記演算処理装置は、ポーリングによって、前記共有メモリにアクセスを行って前記処理の結果を得る

請求項２３に記載のデータ処理機器。

【請求項２７】

前記データ処理装置は、

前記演算処理装置から前記割り込みによって依頼された処理の実行状態を示し、前記演算処理装置によって読まれるフラグを持つ第１のステータスレジスタと、

前記演算処理装置が当該データ処理装置に前記割り込みによって処理を依頼したか否かを示し、前記演算処理装置によって設定されるフラグを持つ第２のステータスレジスタと、

前記処理の結果が書き込まれる前記共有メモリと

を有する請求項２６に記載のデータ処理機器。

【請求項２８】

前記演算処理装置と、前記データ処理装置とを接続するバス

をさらに有する請求項２３に記載のデータ処理機器。

【請求項２９】

前記データ処理装置は、初期プログラムまたは前記割り込みルーチンの実行を終了した後に、低消費電力状態になる

請求項２４に記載のデータ処理機器。

【請求項３０】

前記データ処理装置は、前記演算処理装置から受けた前記割り込みに基づいて、前記コンテンツデータの購入形態または利用形態の決定処理、前記コンテンツデータの再生処理および権威機関からのデータのダウンロード処理のうち少なくとも一の処理に対応する前記割り込みルーチンを実行する

請求項２４に記載のデータ処理機器。

【請求項３１】

前記演算処理装置は、所定のユーザプログラムを実行する

請求項２３に記載のデータ処理機器。

【請求項３２】

データ提供装置が提供したコンテンツデータをデータ配給装置から受け、管理装置によって管理されるデータ処理機器において、

前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、前記データ配給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記デー

タ配給装置による前記モジュールの配給サービスに対しての課金処理を行う第１の処理モジュールと、

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置であって、前記受信したモジュールに格納された権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納されたコンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置と

を有するデータ処理機器。

【請求項３３】

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第１のデータ処理装置と、

前記演算処理装置あるいは前記第１のデータ処理装置から割り込みを受けて、マスタである前記演算処理装置あるいは前記第１のデータ処理装置のスレーブとなって、前記第１のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第２のデータ処理装置と

を有するデータ処理機器。

【請求項３４】

前記演算処理装置、前記第１のデータ処理装置および前記第２のデータ処理装置を接続するバス

をさらに有する請求項３３に記載のデータ処理機器。

【請求項３５】

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第１のデータ処理装置と、

前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第２のデータ処理装置と

を有するデータ処理機器。

【請求項３６】

前記第２のデータ処理装置は、前記記録媒体に対応したメディア鍵データを用いて、前記コンテンツデータの復号および暗号化を行う

請求項３５に記載のデータ処理機器。

【請求項３７】

前記第２のデータ処理装置は、前記記録媒体が相互認証機能を持つ処理回路を搭載している場合に、前記処理回路との間で相互認証を行う

請求項３５に記載のデータ処理機器。

【請求項３８】

所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、

前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第１のデータ処理装置と、

前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第２のデータ処理装置と

を有するデータ処理機器。

【請求項３９】

前記第１のデータ処理装置が前記記録媒体から読み出した前記コンテンツデータを一時的に記憶し、当該記憶したコンテンツデータを前記第２のデータ処理装置に出力する記憶回路

をさらに有する請求項３８に記載のデータ処理機器。

【請求項４０】

前記記憶回路は、耐振動用記憶回路の記憶領域の一部をその記憶領域とする

請求項３９に記載のデータ処理機器。

【請求項４１】

前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第３のデータ処理装置

をさらに有する請求項３８に記載のデータ処理機器。

【請求項４２】

演算処理装置およびデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記データ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性の回路モジュール内で、権利書データが示す取り扱いに基づいて、当該権利書データに対応したコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定の結果を示す履歴データを生成し、前記コンテンツ鍵データを復号する

データ処理方法。

【請求項４３】

前記演算処理装置は、前記割り込みタイプを示す割り込みを受けると、当該割り込みタイプに対応した割り込みルーチンを実行して割り込みを前記データ処理装置に出し、

前記データ処理装置は、前記演算処理装置から受けた前記割り込みによって指

定された処理に対応する割り込みルーチンを実行する

請求項４２に記載のデータ処理方法。

【請求項４４】

前記データ処理装置は、前記処理の結果を前記演算処理装置に割り込みを出して通知する

請求項４２に記載のデータ処理機器。

【請求項４５】

前記データ処理装置は、当該データ処理装置および前記演算処理装置がアクセス可能な共有メモリを有し、

前記演算処理装置は、ポーリングによって、前記共有メモリにアクセスを行って前記処理の結果を得る

請求項４２に記載のデータ処理方法。

【請求項４６】

前記データ処理装置は、前記演算処理装置から前記割り込みによって依頼された処理の実行状態を示す第１のステータスレジスタのフラグを設定し、

前記演算処理装置は、前記第１のステータスレジスタのフラグから、前記データ処理装置の処理の実行状態を把握し、

前記演算処理装置は、前記データ処理装置に前記割り込みによって処理を依頼したことを示す第２のステータスレジスタのフラグに設定し、

前記データ処理装置は、前記第２のステータスレジスタのフラグから、前記演算処理装置が前記割り込みによって処理を依頼したか否かを把握する

請求項４５に記載のデータ処理方法。

【請求項４７】

前記データ処理装置は、初期プログラムまたは前記割り込みルーチンの実行を終了した後に、低消費電力状態になる

請求項４２に記載のデータ処理方法。

【請求項４８】

前記データ処理装置は、前記演算処理装置から受けた前記割り込みに基づいて、前記コンテンツデータの購入形態または利用形態の決定処理、前記コンテンツ

データの再生処理および権威機関からのデータのダウンロード処理のうち少なくとも一の処理に対応する前記割り込みルーチンを実行する

請求項４２に記載のデータ処理方法。

【請求項４９】

前記演算処理装置は、所定のユーザプログラムを実行する

請求項４２に記載のデータ処理方法。

【請求項５０】

演算処理装置、第１のデータ処理装置および第２のデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記第１のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、

前記第２のデータ処理装置は、前記演算処理装置あるいは前記第１のデータ処理装置から割り込みを受けて、マスタである前記演算処理装置あるいは前記第１のデータ処理装置のスレーブとなって、耐タンパ性のモジュール内で、前記第１のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う

データ処理方法。

【請求項５１】

演算処理装置、第１のデータ処理装置および第２のデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記第１のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、

コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、

前記第２のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う

データ処理方法。

【請求項５２】

前記第２のデータ処理装置は、前記記録媒体に対応したメディア鍵データを用いて、前記コンテンツデータの復号および暗号化を行う

請求項５１に記載のデータ処理方法。

【請求項５３】

前記第２のデータ処理装置は、前記記録媒体が相互認証機能を持つ処理回路を搭載している場合に、前記処理回路との間で相互認証を行う

請求項５１に記載のデータ処理方法。

【請求項５４】

演算処理装置、第１のデータ処理装置および第２のデータ処理装置を用いたデータ処理方法において、

前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、

前記第１のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行い、

前記第２のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う

データ処理方法。

【請求項５５】

前記第１のデータ処理装置が前記記録媒体から読み出した前記コンテンツデー

タを記憶回路に一時的に記憶し、当該記憶回路から読み出したコンテンツデータを前記第２のデータ処理装置に出力する

請求項５４に記載のデータ処理方法。

【請求項５６】

前記記憶回路として、耐振動用記憶回路の記憶領域の一部をその記憶領域を用いる

請求項５５に記載のデータ処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、提供されたコンテンツデータに関連する処理を行うデータ処理装置、データ処理機器およびその方法に関する。

【０００２】

【従来の技術】

暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生および記録するデータ提供システムがある。

このようなデータ提供システムの一つに、音楽データを配信する従来のＥＭＤ(Electronic Music Distribution: 電子音楽配信）システムがある。

【０００３】

図１０６は、従来のＥＭＤシステム７００の構成図である。

図１０６に示すＥＭＤシステム７００では、コンテンツプロバイダ７０１ａ，７０１ｂが、サービスプロバイダ７１０に対し、コンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報７０５ａ，７０５ｂ，７０５ｃには、例えば、ＳＣＭＳ(Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ７１０の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【０００４】

サービスプロバイダ７１０は、受信したコンテンツデータ７０４ａ，７０４ｂ，７０４ｃと、著作権情報７０５ａ，７０５ｂ，７０５ｃとをセッション鍵データを用いて復号する。

そして、サービスプロバイダ７１０は、復号したあるいはオフラインで受け取ったコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに、著作権情報７０５ａ，７０５ｂ，７０５ｃを埋め込んで、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを生成する。このとき、サービスプロバイダ７１０は、例えば、著作権情報７０５ａ，７０５ｂ，７０５ｃのうち電子透かし情報をコンテンツデータ７０４ａ，７０４ｂ，７０４ｃに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにＳＣＭＳ情報を埋め込む。

さらに、サービスプロバイダ７１０は、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、鍵データベース７０６から読み出したコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いてそれぞれ暗号化する。その後、サービスプロバイダ７１０は、暗号化されたコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを格納したセキュアコンテナ７２２を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置７０９に存在するＣＡ(Conditional Access)モジュール７１１に送信する。

【０００５】

ＣＡモジュール７１１は、セキュアコンテナ７２２をセッション鍵データを用いて復号する。また、ＣＡモジュール７１１は、電子決済やＣＡなどの課金機能を用いて、サービスプロバイダ７１０の鍵データベース７０６からコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置７０９において、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、それぞれコンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号することが可能になる。

このとき、ＣＡモジュール７１１は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報７２１を生成し、これをセッション鍵データで暗号化した

後に、サービスプロバイダ７１０の権利処理モジュール７２０に送信する。

この場合に、ＣＡモジュール７１１は、サービスプロバイダ７１０が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティー確保とを行う。

【０００６】

サービスプロバイダ７１０は、ＣＡモジュール７１１から課金情報７２１を受信すると、サービスプロバイダ７１０とコンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃとの間で利益配分を行う。

このとき、サービスプロバイダ７１０から、コンテンツプロバイダ７０１ａ，７０１ｂ，７０１ｃへの利益配分は、例えば、ＪＡＳＲＡＣ(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会）を介して行われる。また、ＪＡＳＲＡＣによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【０００７】

また、端末装置７０９では、コンテンツ鍵データＫｃａ，Ｋｃｂ，Ｋｃｃを用いて復号したコンテンツデータ７０７ａ，７０７ｂ，７０７ｃを、ＲＡＭ型の記録媒体７２３などに記録する際に、著作権情報７０５ａ，７０５ｂ，７０５ｃのＳＣＭＳビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ７０７ａ，７０７ｂ，７０７ｃに埋め込まれたＳＣＭＳビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【０００８】

【発明が解決しようとする課題】

ところで、ＳＣＭＳは、コンテンツデータを例えば２世代以上のわたって複製することを禁止するものであり、１世代の複製は無制限に行うことができ、著作権者の保護として不十分であるという問題がある。

【０００９】

また、上述したＥＭＤシステム７００では、サービスプロバイダ７１０が暗号

化されていないコンテンツデータを技術的に自由に扱えるため、コンテンツプロバイダ７０１の関係者はサービスプロバイダ７１０の行為等を監視する必要があり、当該監視の負担が大きいと共に、コンテンツプロバイダ７０１の利益が不当に損なわれる可能性が高いという問題がある。

また、上述したＥＭＤシステム７００では、ユーザの端末装置７０９がサービスプロバイダ７１０から配給を受けたコンテンツデータをオーサリングして他の端末装置などに再配給する行為を規制することが困難であり、コンテンツプロバイダ７０１の利益が不当に損なわれるという問題がある。

【００１０】

本発明は上述した従来技術の問題点に鑑みてなされ、コンテンプロバイダの権利者（関係者）の利益を適切に保護するシステムおよび方法に適用可能なデータ処理装置、データ処理機器およびその方法を提供することを目的とする。

また、本発明は、コンテンプロバイダの権利者の利益を保護するための監査の負担を軽減するシステムおよび方法に適用可能なデータ処理装置、データ処理機器およびその方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】

上述した目的を達成するために、本発明の第１の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置であって、第１のバスと、前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第１のバスに接続された演算処理回路と、前記第１のバスに接続された記憶回路と、第２のバスと、前記第１のバスと前記第２のバスとの間に介在するインターフェイス回路と、　前記第２のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、前記第２のバスに接続された外部バスインターフェイス回路とを耐タンパ性の回路モジュール内に有する。

【００１２】

本発明の第１の観点のデータ処理装置では、例えば、コンテンツデータおよびそれに対応したコンテンツ鍵データおよび権利書データが配給と、暗号化された

コンテンツ鍵データを復号するライセンス鍵データが配給される。

ここで、ライセンス鍵データは、例えば、前記記憶回路に記憶される。

そして、例えば、外部バスインターフェイス回路を介して、外部の演算処理装置から権利処理などを行う指示が出されると、前記演算処理回路において、権利書データに基づいたコンテンツデータの権利処理が行われる。

その後、暗号処理回路において、記憶回路から読み出したライセンス鍵データを用いて、コンテンツ鍵データの復号が行われる。

そして、第１の観点のデータ処理装置は、他の復号装置との間で互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記復号したコンテンツ鍵データおよびコンテンツデータを暗号化し、当該暗号化したコンテンツ鍵データおよびコンテンツデータを前記他の復号装置に送る。

【００１３】

また、本発明の第１の観点のデータ処理装置は、好ましくは、前記インターフェイス回路を第１のインターフェイス回路とした場合に、前記第１のバスは、前記演算処理回路および前記記憶回路に接続された第３のバスと、前記第１のインターフェイス回路に接続された第４のバスとを有し、前記データ処理装置は、

前記第３のバスと前記第４のバスとの間に介在する第２のインターフェイス回路を前記耐タンパ性の回路モジュール内にさらに有する。

【００１４】

また、本発明の第１の観点のデータ処理装置は、好ましくは、第５のバスと、記録媒体またはＩＣカードに搭載された認証機能を持つデータ処理回路との間の通信処理を行い、前記第５のバスに接続された第３のインターフェイス回路と、前記第４のバスと前記第５のバスとの間に介在する第４のインターフェイス回路とを前記耐タンパ性の回路モジュール内にさらに有する。

【００１５】

また、本発明の第１の観点のデータ処理装置は、好ましくは、前記暗号処理回路は、公開鍵暗号回路と、共通鍵暗号回路とを有する。

【００１６】

また、本発明の第１の観点のデータ処理装置は、好ましくは、前記記憶回路は

、当該データ処理装置の秘密鍵データおよび他の装置の公開鍵データを記憶し、前記公開鍵暗号回路は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを対応する前記公開鍵データを用いて検証し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを記録媒体に記録あるいは他の装置に送信するために、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの正当性を示す署名データを前記秘密鍵データを用いて作成し、前記共通鍵暗号回路は、前記コンテンツ鍵データを復号し、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送受信する場合に、前記他の装置との間の前記相互認証によって得られたセッション鍵データを用いて、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを暗号化および復号する。

【００１７】

また、本発明の第１の観点のデータ処理装置は、好ましくは、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データのハッシュ値を生成するハッシュ値生成回路を前記耐タンパ性の回路モジュール内にさらに有し、前記公開鍵暗号回路は、前記ハッシュ値を用いて、前記署名データの検証および前記署名データの作成を行う。

【００１８】

また、本発明の第１の観点のデータ処理装置は、好ましくは、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データを他の装置にオンラインで送信する場合に当該記他の装置との間の相互認証を行うために乱数を生成し、前記第２のバスに接続された乱数生成回路を前記耐タンパ性の回路モジュール内にさらに有する。

【００１９】

また、本発明の第１の観点のデータ処理装置は、好ましくは、前記外部バスインターフェイス回路は、当該データ処理装置が搭載された機器の制御を統括的に行うホスト演算処理装置に接続される。

【００２０】

また、本発明の第１の観点のデータ処理装置は、前記演算処理回路は、前記権利書データが示す取り扱いに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定し、前記決定の結果を示す履歴データを生成する。

【００２１】

また、本発明の第１の観点のデータ処理装置は、好ましくは、前記演算処理回路は、前記購入形態が決定されたときに、当該決定された購入形態に応じた利用制御データを生成し、前記利用制御データに基づいて、前記コンテンツデータの利用を制御する。

【００２２】

また、本発明の第１の観点のデータ処理装置は、好ましくは、前記共通鍵暗号回路は、前記購入形態が決定されたコンテンツデータを記録媒体に記録する場合に、前記コンテンツ鍵データおよび前記利用制御データを、前記記録媒体に対応したメディア鍵データとを用いて暗号化する。

【００２３】

また、本発明の第１の観点のデータ処理装置は、好ましくは、有効期限を持つライセンス鍵データを用いて前記コンテンツ鍵データが暗号化されている場合に、前記記憶回路は、前記ライセンス鍵データを記憶し、前記データ処理装置は、実時間を生成するリアルタイムクロックをさらに有し、前記演算処理回路は、リアルタイムクロックが示す実時間に基づいて、有効期限内の前記ライセンス鍵データを前記記憶回路から読み出し、前記共通鍵暗号回路は、前記読み出されたライセンス鍵データを用いて、前記コンテンツ鍵データを復号する。

【００２４】

また、本発明の第１の観点のデータ処理装置は、好ましくは、前記記憶回路は、ブロック単位でデータの書き込みおよび消去が行われ、前記演算処理回路によって制御され、前記記憶回路に対してのデータの書き込みおよび消去の許否を前記ブロック単位で管理する書き込みロック制御回路を前記耐タンパ性の回路モジュール内にさらに有する。

【００２５】

また、本発明の第２の観点のデータ処理装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータの権利処理を権利書データに基づいて行い、暗号化された前記コンテンツ鍵データを復号するデータ処理装置であって、第１のバスと、前記コンテンツデータの権利処理を前記権利書データに基づいて行い、前記第１のバスに接続された演算処理回路と、前記第１のバスに接続された記憶回路と、第２のバスと、前記第１のバスと前記第２のバスとの間に介在するインターフェイス回路と、前記第２のバスに接続され、前記コンテンツ鍵データの復号を行う暗号処理回路と、前記第２のバスに接続された外部バスインターフェイス回路とを耐タンパ性の回路モジュール内に有し、前記演算処理回路は、前記外部バスインターフェイス回路を介して外部回路から割り込みを受けると、当該外部回路のスレーブとなって当該割り込みによって指定された処理を行い、当該処理の結果を前記外部装置に通知する。

【００２６】

また、本発明の第２の観点のデータ処理装置は、好ましくは、前記演算処理回路は、前記処理の結果を前記外部回路に割り込みを出して通知する。

【００２７】

また、本発明の第２の観点のデータ処理装置は、好ましくは、前記外部バスインターフェイスは、前記演算処理回路および前記外部回路との共有メモリを有し、前記演算処理回路は、当該共有メモリに前記処理の結果を書き込み、当該処理の結果は前記外部回路からのポーリングによって当該外部回路に通知される。

【００２８】

また、本発明の第２の観点のデータ処理装置は、好ましくは、前記外部バスインターフェイスは、前記外部回路から依頼された処理の前記演算処理回路における実行状態を示し、前記演算処理回路によって設定され、前記外部回路によって読まれるフラグを持つ第１のステータスレジスタと、前記外部回路が前記演算処理回路に処理を依頼したか否かを示し、前記外部回路によって設定され、前記演算処理回路によって読まれるフラグを持つ第２のステータスレジスタと、前記処理の結果が書き込まれる記憶回路とを有する。

【００２９】

また、本発明の第２の観点のデータ処理装置は、好ましくは、前記記憶回路は、前記割り込みによって指定される処理を記述した割り込みプログラムを記憶し、前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行して前記処理を行う。

【００３０】

また、本発明の第２の観点のデータ処理装置は、好ましくは、前記記憶回路は、複数の前記割り込みプログラムと、当該割り込みプログラムを実行する際に読み出される複数のサブルーチンとを記憶し、前記演算処理回路は、前記記憶回路から読み出した前記割り込みプログラムを実行する際に、前記記憶回路から必要に応じて前記サブルーチンを読み出して実行する。

【００３１】

また、本発明の第１の観点のデータ処理機器は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置と有するデータ処理機器であって、前記データ処理装置は、権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有する。

【００３２】

また、本発明の第１の観点のデータ処理機器は、好ましくは、前記演算処理装置は、前記割り込みタイプを示す割り込みを受けると、当該割り込みタイプに対応した割り込みルーチンを実行して割り込みを前記データ処理装置に出し、前記データ処理装置は、前記演算処理装置から受けた前記割り込みによって指定された処理に対応する割り込みルーチンを実行する。

【００３３】

また、本発明の第１の観点のデータ処理機器は、好ましくは、前記データ処理

装置は、前記処理の結果を前記演算処理装置に割り込みを出して通知する。

【００３４】

また、本発明の第１の観点のデータ処理機器は、好ましくは、前記データ処理装置は、当該データ処理装置および前記演算処理装置がアクセス可能な共有メモリを有し、前記演算処理装置は、ポーリングによって、前記共有メモリにアクセスを行って前記処理の結果を得る。

【００３５】

また、本発明の第１の観点のデータ処理機器は、好ましくは、前記データ処理装置は、前記演算処理装置から前記割り込みによって依頼された処理の実行状態を示し、前記演算処理装置によって読まれるフラグを持つ第１のステータスレジスタと、前記演算処理装置が当該データ処理装置に前記割り込みによって処理を依頼したか否かを示し、前記演算処理装置によって設定されるフラグを持つ第２のステータスレジスタと、前記処理の結果が書き込まれる前記共有メモリとを有する。

【００３６】

また、本発明の第１の観点のデータ処理機器は、好ましくは、前記データ処理装置は、初期プログラムまたは前記割り込みルーチンの実行を終了した後に、低消費電力状態になる。

【００３７】

また、本発明の第１の観点のデータ処理機器は、好ましくは、前記データ処理装置は、前記演算処理装置から受けた前記割り込みに基づいて、前記コンテンツデータの購入形態または利用形態の決定処理、前記コンテンツデータの再生処理および権威機関からのデータのダウンロード処理のうち少なくとも一の処理に対応する前記割り込みルーチンを実行する。

【００３８】

また、本発明の第１の観点のデータ処理機器は、好ましくは、前記演算処理装置は、所定のユーザプログラムを実行する。

【００３９】

また、本発明の第２の観点のデータ処理機器は、データ提供装置が提供したコ

ンテンツデータをデータ配給装置から受け、管理装置によって管理されるデータ処理機器であって、前記データ提供装置が提供した、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データと、前記データ配給装置が前記コンテンツデータについて付けた価格データとを格納したモジュールを、前記データ配給装置から受信し、共有鍵データを用いて前記受信したモジュールを復号し、前記データ配給装置による前記モジュールの配給サービスに対しての課金処理を行う第１の処理モジュールと、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって所定の処理を行い、当該処理の結果を前記演算処理装置に通知するデータ処理装置であって、前記受信したモジュールに格納された権利書データが示す取り扱いに基づいて、前記受信したモジュールに格納されたコンテンツデータの購入形態および利用形態の少なくとも一方を決定する決定手段と、前記決定の結果を示す履歴データを生成する履歴データ生成手段と、前記コンテンツデータの購入形態の決定処理が行われる際に前記価格データを出力すると共に前記履歴データを前記管理装置に出力する出力手段と、前記コンテンツ鍵データを復号する復号手段とを耐タンパ性の回路モジュール内に有するデータ処理装置とを有する。

【００４０】

また、本発明の第３の観点のデータ処理機器は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第１のデータ処理装置と、前記演算処理装置あるいは前記第１のデータ処理装置から割り込みを受けて、マスタである前記演算処理装置あるいは前記第１のデータ処理装置のスレーブとなって、前記第１のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第２のデータ処理装置とを有する。

【００４１】

また、本発明の第４の観点のデータ処理機器は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第１のデータ処理装置と、前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第２のデータ処理装置とを有する。

【００４２】

また、本発明の第４の観点のデータ処理機器は、好ましくは、前記第２のデータ処理装置は、前記記録媒体に対応したメディア鍵データを用いて、前記コンテンツデータの復号および暗号化を行う。

【００４３】

また、本発明の第４の観点のデータ処理機器は、好ましくは、前記第２のデータ処理装置は、前記記録媒体が相互認証機能を持つ処理回路を搭載している場合に、前記処理回路との間で相互認証を行う。

【００４４】

また、本発明の第５の観点のデータ処理機器は、所定のプログラムを実行し、所定の条件で割り込みを出す演算処理装置と、前記演算処理装置が出した割り込みに応じて、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う耐タンパ性の第１のデータ処理装置と、前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う耐タンパ性の第２のデータ処理装置とを有する。

【００４５】

また、本発明の第５の観点のデータ処理機器は、好ましくは、前記第１のデータ処理装置が前記記録媒体から読み出した前記コンテンツデータを一時的に記憶

し、当該記憶したコンテンツデータを前記第２のデータ処理装置に出力する記憶回路をさらに有する。

【００４６】

また、本発明の第５の観点のデータ処理機器は、好ましくは、前記記憶回路は、耐振動用記憶回路の記憶領域の一部をその記憶領域とする。

【００４７】

また、本発明の第５の観点のデータ処理装置は、好ましくは、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知する耐タンパ性の第３のデータ処理装置をさらに有する。

【００４８】

また、本発明の第１の観点のデータ処理方法は、演算処理装置およびデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記データ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性の回路モジュール内で、権利書データが示す取り扱いに基づいて、当該権利書データに対応したコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定の結果を示す履歴データを生成し、前記コンテンツ鍵データを復号する。

【００４９】

また、本発明の第２の観点のデータ処理方法は、演算処理装置、第１のデータ処理装置および第２のデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記第１のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、前記第２のデータ処理装置は、前記演算処理装置あるいは前記第１のデータ処理装置から割り込みを受けて、マスタであ

る前記演算処理装置あるいは前記第１のデータ処理装置のスレーブとなって、耐タンパ性のモジュール内で、前記第１のデータ処理装置から相互認証を行って得た前記コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う。

【００５０】

また、本発明の第３の観点のデータ処理方法は、演算処理装置、第１のデータ処理装置および第２のデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記第１のデータ処理装置は、前記演算処理装置から割り込みを受けて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いた暗号化されたコンテンツデータの権利処理を行い、当該処理の結果を前記演算処理装置に通知し、前記第２のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行う。

【００５１】

また、本発明の第４の観点のデータ処理方法は、演算処理装置、第１のデータ処理装置および第２のデータ処理装置を用いたデータ処理方法であって、前記演算処理装置は、所定のプログラムを実行し、所定の条件で割り込みを出し、前記第１のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、耐タンパ性のモジュール内で、前記演算処理装置との間で相互認証を行い、前記コンテンツデータが記録媒体に対しての読み出しおよび書き込みを行い、前記第２のデータ処理装置は、前記演算処理装置が出した割り込みに応じて、マスタである前記演算処理装置のスレーブとなって、耐タンパ性のモジュール内で、コンテンツ鍵データを用いたコンテンツデータの復号、並びに前記コンテンツデータの圧縮処理または伸長処理を行う。

【００５２】

【発明の実施の形態】

以下、本発明の実施形態に係わるＥＭＤ(Electronic Music Distribution: 電

子音楽配信）システムについて説明する。

第１実施形態

図１は、本実施形態のＥＭＤシステム１００の構成図である。

本実施形態において、ユーザに配信されるコンテンツ(Content）データとは、情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。

図１に示すように、ＥＭＤシステム１００は、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ（クリアリング・ハウス、以下、ＥＳＣとも記す）１０２およびユーザホームネットワーク１０３を有する。

ここで、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ１０２およびＳＡＭ105_1～105_4が、本発明のデータ提供装置、管理装置およびデータ処理装置にそれぞれ対応している。

先ず、ＥＭＤシステム１００の概要について説明する。

ＥＭＤシステム１００では、コンテンツプロバイダ１０１は、自らが提供しようとするコンテンツのコンテンツデータＣを暗号化する際に用いたコンテンツ鍵データＫｃ、コンテンツデータＣの使用許諾条件などの権利内容を示す権利書(UCP:Usage Control Policy)データ１０６、並びに電子透かし情報の内容および埋め込み位置を示す電子透かし情報管理データを、高い信頼性のある権威機関であるＥＭＤサービスセンタ１０２に送る。

【００５３】

ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１から受けたコンテンツ鍵データＫｃ、権利書データ１０６並びに電子透かし情報鍵データを登録（認証および権威化）する。

また、ＥＭＤサービスセンタ１０２は、対応する期間のライセンス鍵データKD_1～$KD5_6$で暗号化したコンテンツ鍵データＫｃ、権利書データ１０６および自らの署名データなどを格納したキーファイルＫＦを作成し、これをコンテンツプロバイダ１０１に送る。

ここで、当該署名データは、キーファイルＫＦの改竄の有無、キーファイルＫＦの作成者の正当性およびキーファイルＫＦがＥＭＤサービスセンタ１０２にお

いて正規に登録されたことを検証するために用いられる。

【００５４】

また、コンテンツプロバイダ１０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成し、当該生成したコンテンツファイルＣＦと、ＥＭＤサービスセンタ１０２から受けたキーファイルＫＦと、自らの署名データなどを格納したセキュアコンテナ（本発明のモジュール）１０４を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などのパッケージメディアを用いて、ユーザホームネットワーク１０３に配給する。

ここで、セキュアコンテナ１０４内に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【００５５】

ユーザホームネットワーク１０３は、例えば、ネットワーク機器160_1およびＡＶ機器160_2～160_4を有する。

ネットワーク機器160_1は、ＳＡＭ(Secure Application Module) 105_1を内蔵している。

ＡＶ機器160_2～160_4は、それぞれＳＡＭ105_2～105_4を内蔵している。ＳＡＭ105_1～105_4相互間は、例えば、ＩＥＥＥ(Institute of Electrical and Electronics Engineers) １３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。

【００５６】

ＳＡＭ105_1～105_4は、ネットワーク機器160_1がコンテンツプロバイダ１０１からネットワークなどを介してオンラインで受信したセキュアコンテナ１０４、および／または、コンテンツプロバイダ１０１からＡＶ機器160_2～160_4に記録媒体を介してオフラインで供給されたセキュアコンテナ１０４を対応する期間のライセンス鍵データKD_1～KD_3を用いて復号した後に、署名データの検証を行う。

ＳＡＭ105_1～105_4に供給されたセキュアコンテナ１０４は、ネットワ

ーク機器１６０$_1$およびＡＶ機器１６０$_2$～１６０$_4$において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

ＳＡＭ１０５$_1$～１０５$_4$は、上述したセキュアコンテナ１０４の購入・利用の履歴を利用履歴(Usage Log)データ１０８として記録すると共に、購入形態を示す利用制御データ１６６を作成する。

利用履歴データ１０８は、例えば、ＥＭＤサービスセンタ１０２からの要求に応じて、ユーザホームネットワーク１０３からＥＭＤサービスセンタ１０２に送信される。

利用制御データ１６６は、例えば、購入形態が決定される度に、ユーザホームネットワーク１０３からＥＭＤサービスセンタ１０２に送信される。

【００５７】

ＥＭＤサービスセンタ１０２は、利用履歴データ１０８に基づいて、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが決済機関９１に支払った金銭が、ＥＭＤサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１に支払われる。

また、ＥＭＤサービスセンタ１０２は、一定期間毎に、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【００５８】

本実施形態では、ＥＭＤサービスセンタ１０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、ＥＭＤサービスセンタ１０２は、中立の立場にある最高の権威機関であるルート認証局９２に対しての（ルート認証局９２の下層に位置する）セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ１０１およびＳＡＭ１０５$_1$～１０５$_4$において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、ＥＭＤサービスセンタ１０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、ＥＭＤサービスセンタ１０２は、コンテンツプ

ロバイダ１０１の権利書データ１０６を登録して権威化することも、ＥＭＤサービスセンタ１０２の認証機能の一つである。

また、ＥＭＤサービスセンタ１０２は、例えば、ライセンス鍵データKD_1～KD_6などの鍵データの管理を行なう鍵データ管理機能を有する。

また、ＥＭＤサービスセンタ１０２は、権威化した権利書データ１０６に記述された標準小売価格ＳＲＰ(Suggested Retailer' Price)とＳＡＭ１０$5_1$～ＳＡＭ１０$5_4$から入力した利用履歴データ１０８とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ１０１に分配する権利処理（利益分配）機能を有する。

【００５９】

図２は、セキュアコンテナ１０４の概念をまとめた図である。

図２に示すように、セキュアコンテナ１０４には、コンテンツプロバイダ１０１が作成したコンテンツファイルＣＦと、ＥＭＤサービスセンタ１０２が作成したキーファイルＫＦとが格納されている。

コンテンツファイルＣＦには、ヘッダ部およびコンテンツＩＤを含むヘッダデータと、コンテンツ鍵データＫｃを用いた暗号化されたコンテンツデータＣと、これらについてのコンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$を用いた署名データとが格納されている。

キーファイルＫＦには、ヘッダ部およびコンテンツＩＤを含むヘッダデータと、ライセンス鍵データKD_1～KD_6によって暗号化されたコンテンツ鍵データＫｃおよび権利書データ１０６と、これらについてのＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$による署名データとが格納されている。

なお、図２において、権利書データ１０６は、ライセンス鍵データによって暗号化されていなくてもよい。但し、この場合でも、権利書データ１０６には、コンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$を用いた署名データを付加する。

【００６０】

以下、ＥＭＤシステム１００の各構成要素について詳細に説明する。

〔コンテンツプロバイダ１０１〕

コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２との間で通信を行う前に、例えば、自らが生成した公開鍵データ$K_{CP,P}$、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインでＥＭＤサービスセンタ１０２に登録し、自らの識別子（識別番号）ＣＰ＿ＩＤを得る。また、コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２から、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$と、ルート認証局９２の公開鍵データ$K_{R-CA,P}$とを受ける。

【００６１】

コンテンツプロバイダ１０１は、図３（Ａ）に示すコンテンツファイルＣＦと、当該コンテンツファイルＣＦの署名データ$SIG_{6,CP}$と、キーファイルデータベース１１８ｂから読み出した当該コンテンツファイルＣＦに対応する図３（Ｂ）に示すキーファイルＫＦと、当該キーファイルＫＦの署名データ$SIG_{7,CP}$と、記憶部１１９から読み出したコンテンツプロバイダ１０１の公開鍵証明書データCER_{CP}と、当該公開鍵証明書データCER_{CP}の署名データ$SIG_{1,ESC}$とを格納したセキュアコンテナ１０４を生成する。

また、コンテンツプロバイダ１０１は、セキュアコンテナ１０４をオンラインあるいはオフラインで、図１に示すユーザホームネットワーク１０３のネットワーク機器160_1に供給する。

このように、本実施形態では、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}をセキュアコンテナ１０４に格納してユーザホームネットワーク１０３に送信するイン・バンド(In-band) 方式を採用している。従って、ユーザホームネットワーク１０３は、公開鍵証明書CER_{CP}を得るための通信をＥＭＤサービスセンタ１０２との間で行う必要がない。

なお、本発明では、公開鍵証明書CER_{CP}をセキュアコンテナ１０４に格納しないで、ユーザホームネットワーク１０３がＥＭＤサービスセンタ１０２から公開鍵証明書CER_{CP}を得るアウト・オブ・バンド(Out-0f-band) 方式を採用してもよい。

【００６２】

なお、本実施形態では、署名データは、コンテンツプロバイダ１０１、ＥＭＤ

サービスセンタ１０２およびＳＡＭ１０５$_1$～１０５$_4$の各々において、署名を行なう対象となるデータのハッシュ値をとり、自らの秘密鍵データ$K_{CP,S}$，K_{ESC}，K_{SAM1}～K_{SAM4}を用いて作成される。ここで、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの１ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【００６３】

以下、セキュアコンテナ１０４内の各データについて詳細に説明する。

＜署名データＳＩＧ$_{6,CP}$＞

署名データＳＩＧ$_{6,CP}$は、セキュアコンテナ１０４の受信先において、コンテンツファイルＣＦの作成者および送信者の正当性を検証するために用いられる。

＜署名データＳＩＧ$_{7,CP}$＞

署名データＳＩＧ$_{7,CP}$は、セキュアコンテナ１０４の受信先において、キーファイルＫＦの送信者の正当性を検証するために用いられる。なお、セキュアコンテナ１０４の受信先において、キーファイルＫＦの作成者の正当性の検証は、キーファイルＫＦ内の署名データＳＩＧ$_{K1,ESC}$に基づいて行われる。また、署名データＳＩＧ$_{K1,ESC}$は、キーファイルＫＦが、ＥＭＤサービスセンタ１０２に登録されているか否かを検証するためにも用いられる。

【００６４】

＜コンテンツファイルＣＦ＞

図４は、図３（Ａ）に示すコンテンツファイルＣＦをさらに詳細に説明するための図である。

コンテンツファイルＣＦは、図３（Ａ）および図４に示すように、ヘッダデータと、暗号化部１１４から入力したそれぞれコンテンツ鍵データＫｃで暗号化されたメタデータＭｅｔａ、コンテンツデータＣ、Ａ／Ｖ伸長用ソフトウェアＳｏｆｔおよび電子透かし情報モジュール(Watermark Module)WMとを格納している

。

なお、図３（Ａ）は、コンテンツデータＣを伸長するＡＶ圧縮伸長用装置として、ＤＳＰ(Digital Signal Processor)を用いた場合のコンテンツファイルＣＦの構成である。当該ＤＳＰでは、セキュアコンテナ１０４内のＡ／Ｖ伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ１０４内のコンテンツデータＣの伸長および電子透かし情報の埋め込みおよび検出を行う。そのため、コンテンツプロバイダ１０１は任意の圧縮方式および電子透かし情報の埋め込み方式を採用できる。

ＡＶ圧縮伸長用装置としてＡ／Ｖ伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイルＣＦ内にＡ／Ｖ伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【００６５】

ヘッダデータには、図４に示すように、同期信号、コンテンツＩＤ、コンテンツＩＤに対してのコンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$による署名データ、ディレクトリ情報、ハイパーリンク情報、シリアルナンバー、コンテンツファイルＣＦの有効期限並びに作成者情報、ファイルサイズ、暗号の有無、暗号アルゴリズム、署名アルゴリズムに関しての情報、およびディレクトリ情報などに関してのコンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$による署名データが含まれる。

【００６６】

メタデータＭｅｔａには、図４に示すように、商品（コンテンツデータＣ）の説明文、商品デモ宣伝情報、商品関連情報およびこれらについてのコンテンツプロバイダ１０１による署名データが含まれる。

本発明では、図３（Ａ）および図４に示すように、コンテンツファイルＣＦ内にメタデータＭｅｔａを格納して送信する場合を例示するが、メタデータＭｅｔａをコンテンツファイルＣＦ内に格納せずに、コンテンツファイルＣＦを送信する経路とは別の経路でコンテンツプロバイダ１０１から$SAM105_1$などに送信してもよい。

【００６７】

コンテンツデータＣは、例えば、コンテンツマスタソースデータベースから読み出したコンテンツデータに対して、ソース電子透かし情報(Source Watermark)Ｗｓ、コピー管理用電子透かし情報(Copy Control Watermark)Ｗｃ、ユーザ電子透かし情報(User Watermark)Ｗｕおよびリンク用電子透かし情報(Link Watermark)ＷＬなどを埋め込んだ後に、例えば、ＡＴＲＡＣ３(Adaptive Transform Acoustic Coding 3)（商標）などの音声圧縮方式で圧縮され、その後、コンテンツ鍵データＫｃを共通鍵として用い、ＤＥＳ(Data Encryption Standard)やＴｒｉｐｌｅ　ＤＥＳなどの共通鍵暗号化方式で暗号化されたデータである。

ここで、コンテンツ鍵データＫｃは、例えば、乱数発生器を用いて所定ビット数の乱数を発生して得られる。なお、コンテンツ鍵データＫｃは、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データＫｃは、例えば、所定時間毎に更新される。

また、複数のコンテンツプロバイダ１０１が存在する場合に、個々のコンテンツプロバイダ１０１によって固有のコンテンツ鍵データＫｃを用いてもよいし、全てのコンテンツプロバイダ１０１に共通のコンテンツ鍵データＫｃを用いてもよい。

【００６８】

ソース電子透かし情報Ｗｓは、コンテンツデータの著作権者名、ＩＳＲＣコード、オーサリング日付、オーサリング機器ＩＤ(Identification Data)、コンテンツの配給先などの著作権に関する情報である。

コピー管理用電子透かし情報Ｗｃは、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。

ユーザ電子透かし情報Ｗｕには、例えば、セキュアコンテナ１０４の配給元および配給先を特定するためのコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤおよびユーザホームネットワーク１０３のＳＡＭ105_1～105_4の識別子ＳＡＭ＿ID_1～ＳＡＭ＿ID_4が含まれる。

リンク用電子透かし情報(Link Watermark)ＷＬは、例えば、コンテンツデータＣのコンテンツＩＤを含んでいる。

リンク用電子透かし情報ＷＬをコンテンツデータＣに埋め込むことで、例えば、テレビジョンやＡＭ／ＦＭラジオなどのアナログ放送でコンテンツデータＣが配信された場合でも、ユーザからの要求に応じて、ＥＭＤサービスセンタ１０２は、当該コンテンツデータＣを扱っているコンテンツプロバイダ１０１をユーザに紹介できる。すなち、当該コンテンツデータＣの受信先において、電子透かし情報デコーダを利用したコンテンツデータＣに埋め込まれたリンク用電子透かし情報ＷＬを検出し、当該検出したリンク用電子透かし情報ＷＬに含まれるコンテンツＩＤをＥＭＤサービスセンタ１０２に送信することで、ＥＭＤサービスセンタ１０２は当該ユーザに対して、当該コンテンツデータＣを扱っているコンテンツプロバイダ１０１などを紹介できる。

【００６９】

具体的には、例えば、車の中でユーザがラジオを聞きながら、放送中の曲が良いとユーザが思った時点で、所定のボタンを押せば、当該ラジオに内蔵されている電子透かし情報デコーダが、当該コンテンツデータＣに埋め込まれているリンク用電子透かし情報ＷＬに含まれるコンテンツＩＤや当該コンテンツデータＣを登録しているＥＭＤサービスセンタ１０２の通信アドレスなどを検出し、当該検出したデータをメモリスティックなどの半導体メモリやＭＤ(Mini Disk) などの光ディスクなどの可搬メディアに搭載されているメディアＳＡＭに記録する。そして、当該可搬メディアをネットワークに接続されているＳＡＭを搭載したネットワーク機器をセットする。そして、当該ＳＡＭとＥＭＤサービスセンタ１０２とが相互認証を行った後に、メディアＳＡＭに搭載されている個人情報と、上記記録したコンテンツＩＤなどとをネットワーク機器からＥＭＤサービスセンタ１０２に送信する。その後、ネットワーク機器に、当該コンテンツデータＣを扱っているコンテンツプロバイダ１０１などの紹介リストなどを、ＥＭＤサービスセンタ１０２から受信する。

また、その他に、例えば、ＥＭＤサービスセンタ１０２が、ユーザからコンテンツＩＤなどを受信したときに、当該コンテンツＩＤに対応したコンテンツデータＣを提供しているコンテンツプロバイダ１０１に当該ユーザを特定した情報を通知してもよい。この場合に、当該通信を受けたコンテンツプロバイダ１０１は

、当該ユーザが契約者であれば、当該コンテンツデータＣをユーザのネットワーク機器に送信し、当該ユーザが契約者でなければ、自らに関するプロモーション情報をユーザのネットワーク機器に送信してもよい。

【００７０】

なお、後述する第２実施形態では、リンク用電子透かし情報ＷＬに基づいて、ＥＭＤサービスセンタ３０２は、ユーザに、当該コンテンツデータＣを扱っているサービスプロバイダ３１０を紹介できる。

【００７１】

また、本実施形態では、好ましくは、各々の電子透かし情報の内容と埋め込み位置とを、電子透かし情報モジュールWMとして定義し、ＥＭＤサービスセンタ１０２において電子透かし情報モジュールWMを登録して管理する。電子透かし情報モジュールWMは、例えば、ユーザホームネットワーク１０３内のネットワーク機器160_1およびＡＶ機器160_2～160_4が、電子透かし情報の正当性を検証する際に用いられる。

例えば、ユーザホームネットワーク１０３では、ＥＭＤサービスセンタ１０２が管理するユーザ電子透かし情報モジュールに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【００７２】

Ａ／Ｖ伸長用ソフトウェアＳｏｆｔは、ユーザホームネットワーク１０３のネットワーク機器160_1およびＡＶ機器160_2～160_4において、コンテンツファイルＣＦを伸長する際に用いられるソフトウェアであり、例えば、ＡＴＲＡＣ３方式の伸長用ソフトウェアである。

このように、セキュアコンテナ１０４内にＡ／Ｖ伸長用ソフトウェアＳｏｆｔを格納することで、ＳＡＭ105_1～105_4においてセキュアコンテナ１０４内に格納されたＡ／Ｖ伸長用ソフトウェアＳｏｆｔを用いてコンテンツデータＣの伸長を行うことができ、コンテンツデータＣ毎あるいはコンテンツプロバイダ１０１毎にコンテンツデータＣの圧縮および伸長方式をコンテンツプロバイダ１

０１が自由に設定しても、ユーザに多大な負担をかけることはない。

【００７３】

また、コンテンツファイルＣＦには、図４に示すように、ファイルリーダと、秘密鍵データ$K_{cp,S}$によるファイルリーダの署名データとを含むようにしてもよい。このようにすることで、ＳＡＭ１０５$_1$～１０５$_4$において、異系列の複数のセキュアコンテナ１０４から受信したそれぞれ異なるフォーマットのコンテンツファイルＣＦを格納した複数のセキュアコンテナ１０４を効率的に処理できる。

【００７４】

ここで、ファイルリーダは、コンテンツファイルＣＦおよびそれに対応するキーファイルＫＦを読む際に用いられ、これらのファイルの読み込み手順などを示している。

但し、本実施形態では、ＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$～１０５$_4$に、当該ファイルリーダを予め送信している場合を例示する。すなわち、本実施形態では、セキュアコンテナ１０４のコンテンツファイルＣＦは、ファイルリーダを格納していない。

【００７５】

本実施形態では、コンテンツデータＣの圧縮方式、圧縮の有無、暗号化方式（共通鍵暗号化方式および公開鍵暗号化方式の何れの場合も含む）、コンテンツデータＣを得た信号の諸元（サンプリング周波数など）および署名データの作成方式（アルゴリズム）に依存しない形式で、暗号化されたコンテンツデータＣがセキュアコンテナ１０４内に格納されている。すなわち、これらの事項をコンテンツプロバイダ１０１が自由に決定できる。

【００７６】

＜キーファイルＫＦ＞

図５は、図３（Ａ）に示すキーファイルＫＦを詳細に説明するための図である。

本実施形態では、例えば、図６に示すように、コンテンツプロバイダ１０１からＥＭＤサービスセンタ１０２に登録用モジュールＭｏｄ$_2$が送られて登録処理

が行われた後に、例えば６カ月分のキーファイルＫＦがＥＭＤサービスセンタ１０２からコンテンツプロバイダ１０１に送られ、キーファイルデータベースに格納される。このとき、登録用モジュールMod_2およびキーファイルＫＦの送受信時に、コンテンツプロバイダ１０１とＥＭＤサービスセンタ１０２との間の相互認証およびセッション鍵データK_{SES}による暗号化および復号が行われる。

キーファイルＫＦは、コンテンツデータＣ毎に存在し、後述するように、コンテンツファイルＣＦのヘッダ内のディレクトリ構造データＤＳＤによって、対応するコンテンツファイルＣＦとの間でリンク関係が指定されている。

キーファイルＫＦには、図３（Ｂ）および図５に示すように、ヘッダ、コンテンツ鍵データＫｃ、権利書データ（使用許諾条件）１０６、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3および署名データ$SIG_{K1,ESC}$が格納されている。

ここで、コンテンツプロバイダ１０１の秘密鍵データ$K_{ESC,S}$を用いた署名データは、図３（Ｂ）に示すようにキーファイルＫＦに格納される全てのデータに対しての署名データ$_{K1,ESC}$にしてもよいし、図５に示すようにヘッダから鍵ファイルに関する情報までのデータに対しての署名データと、コンテンツ鍵データＫｃおよび権利書データ１０６に対しての署名データと、ＳＡＭプログラム・ダウンロード・コンテナＳＤＣに対しての署名データとを別々に設けてもよい。

コンテンツ鍵データＫｃおよび権利書データ１０６と、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3とは、それぞれ対応する期間のライセンス鍵データKD_1～KD_6を用いて暗号化されている。

なお、権利書データ１０６は、キーファイルＫＦ内に格納しないでもよい。この場合には、例えば、権利書データ１０６はライセンス鍵データによる暗号化を行わずに、署名データを付加する。

【００７７】

ヘッダデータには、図５に示すように、同期信号、コンテンツＩＤ、コンテンツＩＤに対してのコンテンツプロバイダ１０１の秘密鍵データ$K_{ESC,S}$による署名データ、ディレクトリ構造データ、ハイパーリンクデータ、キーファイルＫＦに関する情報、およびディレクトリ構造データ等に対してのコンテンツプロバイ

ダ１０１の秘密鍵データ$K_{ESC,S}$による署名データが含まれる。

なお、ヘッダデータに含める情報としては種々の情報が考えられ、状況に応じて任意に変更可能である。例えば、ヘッダデータに、図７に示すような情報を含めてもよい。

また、コンテンツＩＤには、例えば、図８に示す情報が含まれている。コンテンツＩＤは、ＥＭＤサービスセンタ１０２あるいはコンテンツプロバイダ１０１において作成され、ＥＭＤサービスセンタ１０２において作成された場合には図８に示すようにＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$による署名データが添付され、コンテンツプロバイダ１０１において作成された場合にはコンテンツプロバイダ１０１の秘密鍵データ$K_{CP,S}$が添付される。

コンテンツＩＤは、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２の何れで作成してもよい。

【００７８】

ディレクトリ構造データは、セキュアコンテナ１０４内におけるコンテンツファイルＣＦ相互間の対応関係と、コンテンツファイルＣＦとキーファイルＫＦとの対応関係を示している。

例えば、セキュアコンテナ１０４内にコンテンツファイルCF_1～CF_3と、それらに対応するキーファイルKF_1～KF_3が格納されている場合には、１０図９に示すように、コンテンツファイルCF_1～CF_3相互間のリンクと、コンテンツファイルCF_1～CF_3とキーファイルKF_1～KF_3との間のリンク関係とがディレクトリ構造データによって確立される。

ハイパーリンクデータは、セキュアコンテナ１０４の内外の全てのファイルを対象として、キーファイルＫＦ相互間での階層構造と、コンテンツファイルＣＦとキーファイルＫＦとの対応関係を示している。

具体的には、図１０に示すように、セキュアコンテナ１０４内にコンテンツファイルＣＦおよびキーファイルＫＦ毎のリンク先のアドレス情報とその認証値（ハッシュ値）とを格納し、ハッシュ関数Ｈ（ｘ）を用いて得た自らのアドレス情報のハッシュ値と、相手方の認証値とを比較してリンク関係を検証する。

【００７９】

また、権利書データ１０６は、コンテンツデータＣの運用ルールを定義した記述子（ディスクリプター）であり、例えば、コンテンツプロバイダ１０１の運用者が希望する卸売価格やコンテンツデータＣの複製ルールなどが記述されている。

具体的には、権利書データ１０６には、図５に示すように、コンテンツＩＤ、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、権利書データ１０６の有効期限、ＥＭＤサービスセンタ１０２の通信アドレス、利用空間調査情報、卸売価格情報ＳＲＰ(Suggested Retailer' Price)、取扱方針、取扱制御情報(Usage Control)、商品デモ（試聴）の取扱制御情報およびそれらについての署名データなどが含まれる。

ここで、取扱制御情報は、例えば、再配付(Re-Distribution)、再生課金(Pay Per Use)、完全買い切り(Sell Through)、時間制限買い切り(Time Limited Sell Through)、回数制限買い切り(Shell Through Pay Per Play N)、時間課金(Pay Per Time)、ＳＣＭＳ機器への再生課金、ブロック課金(Pay Per Block)などの購入形態のうち許諾された購入形態を示す情報である。

【００８０】

なお、後述する第２実施形態のように、サービスプロバイダ３１０を介してユーザホームネットワーク３０３にセキュアコンテナ３０４を送信する場合には、権利書データ１０６には、コンテンツプロバイダ３０１がセキュアコンテナ１０４を提供するサービスプロバイダ３１０の識別子ＳＰ＿ＩＤが含まれる。

【００８１】

また、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3には、図５に示すように、ＳＡＭ105_1～105_4内でプログラムのダウンロードを行なう際に用いられるダウンロードの手順を示すダウンロード・ドライバと、権利書データ（ＵＣＰ）Ｕ１０６のシンタックス（文法）を示すＵＣＰ－Ｌ(Label)．Ｒ(Reader)などのラベルリーダと、ＳＡＭ105_1～105_4に内蔵された記憶部１９２（マスクＲＯＭ１１０４、不揮発性メモリ１１０５などのフラッシュＥＥＰＲＯＭ）の書き換えおよび消去をブロック単位でロック状態／非ロック状態

にするためのロック鍵データと、それらについての署名データとが含まれる。ＳＡＭ１０５$_1$～１０５$_4$のマスクＲＯＭ１１０４および不揮発性メモリ１１０５では、ロック鍵データに基づいて、記憶データの書き換えおよび消去を許可するか否かをブロック単位で制御する。

【００８２】

以下、コンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を供給する形態について説明する。

コンテンツプロバイダ１０１は、前述したように、セキュアコンテナ１０４を、オフラインおよび／またはオンラインでユーザホームネットワーク１０３に供給する。

コンテンツプロバイダ１０１は、オンラインで、セキュアコンテナ１０４をユーザホームネットワーク１０３のネットワーク機器１６０$_1$に供給する場合には、ネットワーク機器１６０$_1$との間で相互認証を行ってセッション鍵（共通鍵）データK_{SES}を共有し、セキュアコンテナ１０４を当該セッション鍵データK_{SES}を用いて暗号化してＥＭＤサービスセンタ１０２に送信する。セッション鍵データK_{SES}は、相互認証を行う度に新たに生成される。

このとき、セキュアコンテナ１０４を送信する通信プロコトルとして、デジタル放送であればＭＨＥＧ(Multimedia and Hypermedia information coding Experts Group)プロトコルを用い、インターネットであればＸＭＬ／ＳＭＩＬ／ＨＴＭＬ(Hyper TextMarkup Language) を用い、これらの通信プロトコル内に、セキュアコンテナ１０４を、符号化方式に依存しない形式でトンネリングして埋め込む。

従って、通信プロコトルとセキュアコンテナ１０４との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ１０４のフォーマットを柔軟に設定できる。

なお、コンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を送信する際に用いる通信プロトコルは、上述したものには限定されず任意である。

本実施形態では、コンテンツプロバイダ１０１、ＥＭＤサービスセンタ１０２

およびネットワーク機器１６０$_1$に内蔵された相互間で通信を行うためのモジュールとして、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【００８３】

また、コンテンツプロバイダ１０１は、オフラインで、セキュアコンテナ１０４をユーザホームネットワーク１０３に供給する場合には、以下に示すようなＲＯＭ型あるいはＲＡＭ型の記録媒体にセキュアコンテナ１０４を記録して、当該記録媒体を所定の流通経路を経てユーザホームネットワーク１０３に供給する。

図１１は、本実施形態で用いられるＲＯＭ型の記録媒体１３０$_1$を説明するための図である。

図１１に示すように、ＲＯＭ型の記録媒体１３０$_1$は、ＲＯＭ領域１３１、セキュアＲＡＭ領域１３２およびメディアＳＡＭ１３３を有する。

ＲＯＭ領域１３１には、図３（Ａ）に示したコンテンツファイルＣＦが記憶されている。

また、セキュアＲＡＭ領域１３２は、記憶データに対してのアクセスに所定の許可（認証）が必要な領域であり、図３（Ｂ）、（Ｃ）に示したキーファイルＫＦおよび公開鍵証明書データCER_{CP}と機器の種類に応じて固有の値を持つ記録用鍵データK_{STR}とを引数としてＭＡＣ(Message Authentication Code) 関数を用いて生成した署名データと、当該キーファイルＫＦおよび公開鍵証明書データCER_{CP}とを記録媒体に固有の値を持つメディア鍵データK_{MED}を用いて暗号化したデータとが記憶される。

また、セキュアＲＡＭ領域１３２には、例えば、不正行為などで無効となったコンテンツプロバイダ１０１およびＳＡＭ105_1～105_5を特定する公開鍵証明書破棄データ（リボケーションリスト）が記憶される。

本実施形態で用いられるメディアＳＡＭおよび後述するメディア・ドラブＳＡＭ２６０では、これら相互間で通信を行う際に、自らが持つリボケーションリストと相手方が持つリボケーションリストとの作成時を比較し、自らが持つリボケーションリストの作成時が前の場合には、相手方が持つリボケーションリストによって自らのリボケーションリストを更新する。

また、セキュアＲＡＭ領域１３２には、後述するようにユーザホームネットワーク１０３のＳＡＭ105_1～105_4においてコンテンツデータＣの購入・利用形態が決定されたときに生成される利用制御状態（ＵＣＳ）データ１６６などが記憶される。これにより、利用制御データ１６６がセキュアＲＡＭ領域１３２に記憶されることで、購入・利用形態が決定したＲＯＭ型の記録媒体130_1となる。

メディアＳＡＭ１３３には、例えば、ＲＯＭ型の記録媒体130_1の識別子であるメディアＩＤと、メディア鍵データK_{MED}とが記憶されている。

メディアＳＡＭ１３３は、例えば、相互認証機能を有している。

【００８４】

本実施形態で用いるＲＯＭ型の記録媒体としては、例えば、図１１に示すものの他に、図１２に示すＲＯＭ型の記録媒体130_2および図１３に示すＲＯＭ型の記録媒体130_3なども考えられる。

図１２に示すＲＯＭ型の記録媒体130_2は、ＲＯＭ領域１３１と認証機能を有するメディアＳＡＭ１３３とを有し、図１１に示すＲＯＭ型の記録媒体130_1のようにセキュアＲＡＭ領域１３２を備えていない。ＲＯＭ型の記録媒体130_2を用いる場合には、ＲＯＭ領域１３１にコンテンツファイルＣＦを記録し、メディアＳＡＭ１３３にキーファイルＫＦを記憶する。

また、図１３に示すＲＯＭ型の記録媒体130_3は、ＲＯＭ領域１３１およびセキュアＲＡＭ領域１３２を有し、図１１に示すＲＯＭ型の記録媒体130_1のようにメディアＳＡＭ１３３を有していない。ＲＯＭ型の記録媒体130_3を用いる場合には、ＲＯＭ領域１３１にコンテンツファイルＣＦを記録し、セキュアＲＡＭ領域１３２にキーファイルＫＦを記録する。また、ＲＯＭ型の記録媒体130_3を用いる場合には、ＳＡＭとの間で相互認証は行わない。

また、本実施形態ではＲＯＭ型の記録媒体の他にＲＡＭ型の記録媒体も用いられる。

【００８５】

本実施形態で用いるＲＡＭ型の記録媒体としては、例えば図１４に示すように、メディアＳＡＭ１３３、セキュアＲＡＭ領域１３２およびセキュアでないＲＡ

M領域１３４を有するＲＡＭ型の記録媒体130_4がある。ＲＡＭ型の記録媒体130_4では、メディアＳＡＭ１３３は認証機能を持ち、キーファイルＫＦを記憶する。また、ＲＡＭ領域１３４には、コンテンツファイルＣＦが記録される。

また、本実施形態で用いるＲＡＭ型の記録媒体としては、その他に、図１５に示すＲＡＭ型の記録媒体1350_5および図１６に示すＲＡＭ型の記録媒体130_6なども考えられる。

図１５に示すＲＡＭ型の記録媒体130_5は、セキュアでないＲＡＭ領域１３４と認証機能を有するメディアＳＡＭ１３３とを有し、図１４に示すＲＡＭ型の記録媒体130_4のようにセキュアＲＡＭ領域１３２を備えていない。ＲＡＭ型の記録媒体130_5を用いる場合には、ＲＡＭ領域１３４にコンテンツファイルＣＦを記録し、メディアＳＡＭ１３３にキーファイルＫＦを記憶する。

また、図１６に示すＲＡＭ型の記録媒体130_6は、セキュアＲＡＭ領域１３２およびセキュアでないＲＡＭ領域１３４を有し、図１４に示すＲＡＭ型の記録媒体130_4のようにメディアＳＡＭ１３３を有していない。ＲＡＭ型の記録媒体130_6を用いる場合には、ＲＡＭ領域１３４にコンテンツファイルＣＦを記録し、セキュアＲＡＭ領域１３２にキーファイルＫＦを記録する。また、ＲＡＭ型の記録媒体130_6を用いる場合には、ＳＡＭとの間で相互認証は行わない。

【００８６】

ここで、コンテンツプロバイダ１０１からユーザホームネットワーク１０３へのコンテンツデータＣの配給は、上述したように記録媒体130_1を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ１０６が格納された共通の形式のセキュアコンテナ１０４を用いる。従って、ユーザホームネットワーク１０３のＳＡＭ105_1～105_4では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ１０６に基づいた権利処理を行なうことができる。

【００８７】

また、上述したように、本実施形態では、セキュアコンテナ１０４内に、コンテンツ鍵データＫｃで暗号化されたコンテンツデータＣと、当該暗号化を解くためのコンテンツ鍵データＫｃとを同封するイン・バンド(In-Band) 方式を採用し

ている。イン・バンド方式では、ユーザホームネットワーク１０３の機器で、コンテンツデータＣを再生しようとするときに、コンテンツ鍵データＫｃを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データＫｃはライセンス鍵データKD_1～KD_6で暗号化されているが、ライセンス鍵データKD_1～KD_6は、ＥＭＤサービスセンタ１０２で管理されており、ユーザホームネットワーク１０３のＳＡＭ105_1～105_5に事前に（ＳＡＭ105_1～105_4がＥＭＤサービスセンタ１０２に初回にアクセスする際に）配信されているので、ユーザホームネットワーク１０３では、ＥＭＤサービスセンタ１０２との間をオンラインで接続することなく、オフラインで、コンテンツデータＣの利用が可能になる。

なお、本発明は、後述するようにコンテンツデータＣとコンテンツ鍵データＫｃとを別々に、ユーザホームネットワーク１０３に供給するアウト・オブ・バンド(Out-Of-Band) 方式を採用できる柔軟性を有している。

【００８８】

以下、コンテンツプロバイダ１０１におけるセキュアコンテナ１０４の作成に係わる処理の流れを説明する。

図１７，図１８，図１９は、当該処理の流れを説明するためのフローチャートである。

ステップＳ１７－１：コンテンツプロバイダ１０１の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、ＥＭＤサービスセンタ１０２に登録処理を行い、グローバルユニークな識別子ＣＰ＿ＩＤを得ている。また、コンテンツプロバイダ１０１は、予め自らの公開鍵証明書データCER_{CP}をＥＭＤサービスセンタ１０２から得ている。

ステップＳ１７－２：コンテンツプロバイダ１０１は、新しくオーサリングするコンテンツデータや、既に保管されているレガシーコンテンツデータなどのコンテンツマスタソースをデジタル化し、さらにコンテンツＩＤを割り振り、コンテンツマスタソースデータベースに格納して一元的に管理する。

ステップＳ１７－３：コンテンツプロバイダ１０１は、ステップＳ１７－２において一元的に管理した各々のコンテンツマスタソースにメタデータＭｅｔａを

作成し、これをメタデータデータベースに格納して管理する。

【００８９】

ステップＳ１７－４：コンテンツプロバイダ１０１は、コンテンツマスタソースデータベースからコンテンツマスタソースであるコンテンツデータを読み出して電子透かし情報を埋め込む。

ステップＳ１７－５：コンテンツプロバイダ１０１は、ステップＳ１７－４で埋め込んだ電子透かし情報の内容と埋め込み位置とを所定のデータベースに格納する。

ステップＳ１７－６：電子透かし情報が埋め込まれたコンテンツデータを圧縮する。

ステップＳ１７－７：コンテンツプロバイダ１０１は、ステップＳ１７－６で圧縮したコンテンツデータを伸長してコンテンツデータを生成する。

ステップＳ１７－８：コンテンツプロバイダ１０１は、伸長したコンテンツデータの聴覚検査を行う。

ステップＳ１７－９：コンテンツプロバイダ１０１は、コンテンツデータに埋め込まれた電子透かし情報を、ステップＳ１７－５でデータベースに格納した埋め込み内容および埋め込み位置に基づいて検出する。

そして、コンテンツプロバイダ１０１は、聴覚検査および電子透かし情報の検出の双方が成功した場合には、ステップＳ１７－１０の処理を行い、何れか一方が失敗した場合にはステップＳ１７－４の処理を繰り返す。

【００９０】

ステップＳ１７－１０：コンテンツプロバイダ１０１は、乱数を発生してコンテンツ鍵データＫｃを生成し、これを保持する。また、コンテンツプロバイダ１０１は、ステップＳ１７－６で圧縮したコンテンツデータを、コンテンツ鍵データＫｃを用いて暗号化する。

【００９１】

ステップＳ１７－１１：コンテンツプロバイダ１０１は、図３（Ａ）に示すコンテンツファイルＣＦを作成し、これをコンテンツファイルデータベースに格納する。

【００９２】

ステップＳ１７－１２：コンテンツプロバイダ１０１は、コンテンツデータＣについての権利書データ１０６を作成する。

ステップＳ１７－１３：コンテンツプロバイダ１０１は、ＳＲＰを決定する。

ステップＳ１７－１４：コンテンツプロバイダ１０１は、コンテンツＩＤ、コンテンツ鍵データＫｃおよび権利書データ１０６をＥＭＤサービスセンタ１０２に出力する。

ステップＳ１７－１５：コンテンツプロバイダ１０１は、ライセンス鍵データKD_1～KD_3で暗号化されたキーファイルＫＦをＥＭＤサービスセンタ１０２から入力する。

ステップＳ１７－１６：コンテンツプロバイダ１０１は、入力したキーファイルＫＦをキーファイルデータベースに格納する。

【００９３】

ステップＳ１７－１７：コンテンツプロバイダ１０１は、コンテンツファイルＣＦとキーファイルＫＦとのリンク関係をハイパーリンクで結ぶ。

ステップＳ１７－１８：コンテンツプロバイダ１０１は、コンテンツファイルＣＦのハッシュ値をとり、秘密鍵データ$K_{CP,S}$を用いて署名データ$SIG_{6,CP}$を生成する。また、コンテンツプロバイダ１０１は、キーファイルＫＦのハッシュ値をとり、秘密鍵データ$K_{CP,S}$を用いて署名データ$SIG_{7,CP}$を生成する。

【００９４】

ステップＳ１７－１９：コンテンツプロバイダ１０１は、図３に示すように、コンテンツファイルＣＦ、キーファイルＫＦ、公開鍵証明書データCER_{CP}、署名データ$SIG_{6,CP}$，$SIG_{7,CP}$，$SIG_{1,ESC}$を格納したセキュアコンテナ１０４を作成する。

【００９５】

ステップＳ１７－２０：複数のセキュアコンテナを用いたコンポジット形式でコンテンツデータを提供する場合には、ステップＳ１７－１～Ｂ１９の処理を繰り返して各々のセキュアコンテナ１０４を作成し、コンテンツファイルＣＦとキーファイルＫＦとの間のリンク関係と、コンテンツファイルＣＦ相互間のリンク

関係とをハイパーリンクなどを用いて結ぶ。

ステップＳ１７－２１：コンテンツプロバイダ１０１は、作成したセキュアコンテナ１０４をセキュアコンテナデータベースに格納する。

【００９６】

〔ＥＭＤサービスセンタ１０２〕

図２０は、ＥＭＤサービスセンタ１０２の主な機能を示す図である。

ＥＭＤサービスセンタ１０２は、主に、図２０に示すように、ライセンス鍵データをコンテンツプロバイダ１０１およびＳＡＭ１０５$_1$～１０５$_4$に供給する処理と、公開鍵証明書データＣＥＲ$_{CP}$，ＣＥＲ$_{SAM1}$～ＣＥＲ$_{SAM4}$の発行処理と、キーファイルＫＦの発行処理、利用履歴データ１０８に基づいた決済処理（利益分配処理）とを行う。

【００９７】

＜ライセンス鍵データの供給処理＞

先ず、ＥＭＤサービスセンタ１０２からユーザホームネットワーク１０３内のＳＡＭ１０５$_1$～１０５$_4$にライセンス鍵データを送信する際の処理の流れを説明する。

ＥＭＤサービスセンタ１０２では、所定期間毎に、例えば、３カ月分のライセンス鍵データＫＤ$_1$～ＫＤ$_3$を鍵データベースから読み出して、各々のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データＫ$_{ESC,S}$を用いて、それぞれに対応する署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD3,ESC}$を作成する。

そして、ＥＭＤサービスセンタ１０２は、３カ月分のライセンス鍵データＫＤ$_1$～ＫＤ$_3$およびそれらの署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD3,ESC}$を、ＳＡＭ１０５$_1$～１０５$_4$と間の相互認証で得られたセッション鍵データＫ$_{SES}$を用いて暗号化した後に、ＳＡＭ１０５$_1$～１０５$_4$に送信する。

また、同様に、ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１に、例えば、６カ月分のライセンス鍵データＫＤ$_1$～ＫＤ$_6$を送信する。

【００９８】

＜公開鍵証明書データの発行処理＞

次に、ＥＭＤサービスセンタ１０２がコンテンツプロバイダ１０１から、公開

鍵証明書データCER_{CP}の発行要求を受けた場合の処理を説明する。

ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、公開鍵データ$K_{CP,P}$および署名データ$SIG_{9,CP}$をコンテンツプロバイダ１０１から受信すると、これらを、コンテンツプロバイダ１０１との間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。

そして、当該復号した署名データ$SIG_{9,CP}$の正当性を検証した後に、識別子ＣＰ＿ＩＤおよび公開鍵データ$K_{CP,P}$に基づいて、当該公開鍵証明書データの発行要求を出したコンテンツプロバイダ１０１がＣＰデータベースに登録されているか否かを確認する。

そして、ＥＭＤサービスセンタ１０２は、当該コンテンツプロバイダ１０１のＸ．５０９形式の公開鍵証明書データCER_{CP}を証明書データベースから読み出し、公開鍵証明書データCER_{CP}のハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて、署名データ$SIG_{1,ESC}$を作成する。

そして、ＥＭＤサービスセンタ１０２は、公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$を、コンテンツプロバイダ１０１との間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【００９９】

なお、ＥＭＤサービスセンタ１０２が$SAM105_1$から、公開鍵証明書データCER_{SAM1}の発行要求を受けた場合の処理も、$SAM105_1$との間で処理が行われる点を除いて、公開鍵証明書データCER_{CP}の発行要求を受けた場合の処理と同じである。公開鍵証明書データCER_{CP}も、Ｘ．５０９形式で記述されている。

なお、本発明では、ＥＭＤサービスセンタ１０２は、例えば、$SAM105_1$の出荷時に、$SAM105_1$の秘密鍵データ$K_{SAM1,S}$および公開鍵データ$K_{SAM1,P}$を$SAM105_1$の記憶部に記憶する場合には、当該出荷時に、公開鍵データ$K_{SAM1,P}$の公開鍵証明書データCER_{SAM1}を作成してもよい。

このとき、当該出荷時に、公開鍵証明書データCER_{SAM1}を、$SAM105_1$の記憶部に記憶してもよい。

【０１００】

＜キーファイルＫＦの発行処理＞

ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１から図６に示す登録用モジュールＭｏｄ$_2$を受信すると、コンテンツプロバイダ１０１と間の相互認証で得られたセッション鍵データK_{SES}を用いて登録用モジュールＭｏｄ$_2$を復号する。

そして、ＥＭＤサービスセンタ１０２は、鍵データベースから読み出した公開鍵データ$K_{cp,P}$を用いて、署名データ$SIG_{M1,CP}$の正当性を検証する。

次に、ＥＭＤサービスセンタ１０２は、登録用モジュールＭｏｄ$_2$に格納された権利書データ１０６、コンテンツ鍵データＫｃ、電子透かし情報管理データＷＭおよびＳＲＰを、権利書データベースに登録する。

【０１０１】

次に、ＥＭＤサービスセンタ１０２は、鍵サーバから読み出した対応する期間のライセンス鍵データKD_1～KD_6を用いて、コンテンツ鍵データＫｃおよび権利書データ１０６と、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3とを暗号化する。

次に、ＥＭＤサービスセンタ１０２は、ヘッダデータと、コンテンツ鍵データＫｃおよび権利書データ１０６と、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3との全体に対してハッシュ値をとり、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いて署名データ$SIG_{K1,ESC}$を作成する。

次に、ＥＭＤサービスセンタ１０２は、図３（Ｂ）に示すキーファイルＫＦを作成し、これをＫＦデータベースに格納する。

次に、ＥＭＤサービスセンタ１０２は、ＫＦデータベースにアクセスを行って得たキーファイルＫＦを、コンテンツプロバイダ１０１と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ１０１に送信する。

【０１０２】

＜決算処理＞

次に、ＥＭＤサービスセンタ１０２において行なう決済処理について説明する

。

ＥＭＤサービスセンタ１０２は、ユーザホームネットワーク１０３の例えばＳＡＭ１０５$_1$から利用履歴データ１０８およびその署名データＳＩＧ$_{200,SAM1}$を入力すると、利用履歴データ１０８および署名データＳＩＧ$_{200,SAM1}$を、ＳＡＭ１０５$_1$との間の相互認証によって得られたセッション鍵データＫ$_{SES}$を用いて復号し、ＳＡＭ１０５$_1$の公開鍵データＫ$_{SAM1}$による署名データＳＩＧ$_{200,SAM1}$の検証を行う。

【０１０３】

図２１は、利用履歴データ１０８に記述されるデータを説明するための図である。

図２１に示すように、利用履歴データ１０８には、例えば、セキュアコンテナ１０４に格納されたコンテンツデータＣに対してＥＭＤサービスセンタ１０２によってグローバルユニークに付された識別子であるＥＳＣ＿コンテンツＩＤ、当該コンテンツデータＣに対してコンテンツプロバイダ１０１によって付された識別子であるＣＰ＿コンテンツＩＤ、セキュアコンテナ１０４の配給を受けたユーザの識別子であるユーザＩＤ、当該ユーザのユーザ情報、セキュアコンテナ１０４の配給を受けたＳＡＭ１０５$_1$～１０５$_4$の識別子ＳＡＭ＿ＩＤ、当該ＳＡＭが属するホームネットワークグループの識別子であるＨＮＧ＿ＩＤ、ディスカウント情報、トレーシング情報、プライスタグ、当該コンテンツデータを提供したコンテンツプロバイダ１０１の識別子ＣＰ＿ＩＤ、紹介業者（ポータル:Portal）ＩＤ、ハードウェア提供者ＩＤ、セキュアコンテナ１０４を記録した記録媒体の識別子Ｍｅｄｉａ＿ＩＤ、セキュアコンテナ１０４の提供に用いられた例えば圧縮方法などの所定のコンポーネントの識別子であるコンポーネントＩＤ、セキュアコンテナ１０４のライセンス所有者の識別子ＬＨ＿ＩＤ、セキュアコンテナ１０４についての決済処理を行うＥＭＤサービスセンタ１０２の識別子ＥＳＣ＿ＩＤなどが記述されている。

なお、後述する第２実施形態では、利用履歴データ３０８には、上述した利用履歴データ１０８に記述されたデータに加えて、当該コンテンツデータＣに対してサービスプロバイダ３１０によって付された識別子であるＳＰ＿コンテンツＩ

Ｄと、当該コンテンツデータＣを配給したサービスプロバイダ３１０の識別子ＳＰ＿ＩＤとが記述されている。

【０１０４】

ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク１０３のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ１０７および決済請求権データ１５２を作成する。当該分配率表は、例えば、セキュアコンテナ１０４に格納されたコンテンツデータ毎に作成される。

【０１０５】

次に、ＥＭＤサービスセンタ１０２は、利用履歴データ１０８と、権利書データベースから読み出した権利書データ１０６に含まれる標準小売価格データＳＲＰおよび販売価格とに基づいて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を生成する。

ここで、決済請求権データ１５２は、当該データに基づいて、決済機関９１に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

【０１０６】

次に、ＥＭＤサービスセンタ１０２は、決済請求権データ１５２およびその署名データSIG_{99}を、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図１に示すペイメントゲートウェイ９０を介して決済機関９１に送信する。

これにより、決済請求権データ１５２に示される金額の金銭が、コンテンツプロバイダ１０１に支払われる。

また、ＥＭＤサービスセンタ１０２は、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【０１０７】

〔ユーザホームネットワーク１０３〕

ユーザホームネットワーク１０３は、図１に示すように、ネットワーク機器１６０$_1$およびA／V機器１６０$_2$～１６０$_4$を有している。

ネットワーク機器１６０$_1$は、ＳＡＭ１０５$_1$を内蔵している。また、ＡＶ機器１６０$_2$～１６０$_4$は、それぞれＳＡＭ１０５$_2$～１０５$_4$を内蔵している。

ＳＡＭ１０５$_1$～１０５$_4$の相互間は、例えば、ＩＥＥＥ１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。

なお、ＡＶ機器１６０$_2$～１６０$_4$は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器１６０$_1$のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク１０３は、ネットワーク機能を有していないＡＶ機器のみを有していてもよい。

【０１０８】

以下、ネットワーク機器１６０$_1$について説明する。

図２２は、ネットワーク機器１６０$_1$の構成図である。

図２２に示すように、ネットワーク機器１６０$_1$は、ＳＡＭ１０５$_1$、通信モジュール１６２、ＡＶ圧縮・伸長用ＳＡＭ１６３、操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９、外部メモリ２０１およびホストＣＰＵ８１０を有する。

ここで、ホストＣＰＵ８１０はネットワーク機器１６０$_1$内の処理を統括的に制御しており、ホストＣＰＵ８１０とＳＡＭ１０５$_1$とは、それぞれマスタ(Master)とスレーブ(Slave)の関係にある。

以下、ホストＣＰＵ８１０とＳＡＭ１０５$_1$との関係を詳細に説明する。

図２３は、ホストＣＰＵ８１０とＳＡＭ１０５$_1$との関係を説明するための図である。

図２３に示すように、ネットワーク機器１６０$_1$では、ホストＣＰＵバス１０００を介して、ホストＣＰＵ８１０とＳＡＭ１０５$_1$とが接続されている。

ホストＣＰＵ８１０は、例えばユーザによる操作部１６５の操作に応じて複数の割り込みタイプの中から一の割り込みタイプが選択された場合に、当該選択さ

れた割り込みタイプを示す外部割り込み（ハードウェア割り込み）Ｓ１６５を受ける。

また、ホストＣＰＵ８１０は、外部割り込みＳ１６５を受け、当該外部割り込みＳ１６５に対応するタスクがＳＡＭ１０５$_1$が実行すべきものである場合に、当該タスクを指定した内部割り込み（ソフトウェア割り込み）Ｓ８１０を、ホストＣＰＵバス１０００を介してＳＡＭ１０５$_1$に出す。

【０１０９】

ＳＡＭ１０５$_1$は、ホストＣＰＵ８１０からＩ／Ｏデバイスとして認識され、ホストＣＰＵ８１０からのファンクションコールである内部割り込みＳ８１０を受けて、要求に応じたタスクを実行し、当該タスクの実行結果をホストＣＰＵ８１０に返す。

ＳＡＭ１０５$_1$が実行するタスクは、主に、コンテンツデータの購入処理（課金処理）、署名検証処理、相互認証処理、コンテンツデータの再生処理、更新処理、登録処理、ダウンロード処理などに関するものであり、これらのタスク群はＳＡＭ１０５$_1$内で外部から遮蔽された形で処理され、ホストＣＰＵ８１０は当該処理内容をモニタできない。

ホストＣＰＵ８１０は、どのようなイベントのときにＳＡＭ１０５$_1$にタスクを依頼するかを予め把握している。具体的には、ホストＣＰＵ８１０は、ユーザによる外部キーデバイスなどの操作部１６５の操作に応じた外部割り込みＳ１６５を受けて、当該割り込みによって実行すべきタスクがＳＡＭ１０５$_1$が実行するタスクであると判断すると、ホストＣＰＵバス１０００を介してＳＡＭ１０５$_1$に内部割り込みＳ８１０をかけ、ＳＡＭ１０５$_1$に当該タスクを実行させる。

【０１１０】

ここで、コマンダーおよびキーボードなどの外部キーデバイスなどのホストＣＰＵ８１０に対してのＩ／Ｏデバイスに相当するものから受ける割り込みは、ホストＣＰＵ８１０が実行するユーザプログラムの内容とは全く非同期なイベントによって生じる割り込みであり、通常、これらを“ハードウエア割り込み”あるいは”外部割り込み”と呼んでいる。

ホストＣＰＵ８１０が、コンテンツの視聴および購入時に受ける割り込みは、

ハードウェア割り込みである。このとき、ハードウェア割り込みを発生するＩ／Ｏデバイスは、例えば、ネットワーク機器１６０$_1$のボタン類やＧＵＩ(Graphical User Interface)のアイコンなどのキーデバイスである。本実施形態では、これらのＩ／Ｏデバイスを操作部１６５としている。

【０１１１】

一方、ホストＣＰＵ８１０によるユーザプログラム（プログラム）の実行に基づいて発生する割り込みは、“ソフトウェア割り込み”または”内部割り込みと呼ばれる。

【０１１２】

外部割り込みＳ１６５は、通常、その割り込み信号を、ホストＣＰＵバス１０００とは別に設けられた外部割り込み専用線を介して操作部１６５からホストＣＰＵ８１０に出力している。

外部割り込みＳ１６５の種類は、割り込みが発生するＩ／Ｏデバイスに番号を持たせることで区別される。例えば、キーボードなどでは、全てのボタン（当該番号を割り込みタイプと呼ぶ）に番号が割り当てられ、ボタンが押されると、当該ボタンが押下されたことを外部割り込み専用線を介して操作部１６５からホストＣＰＵ８１０に通知し、当該押下されたボタンの番号をＩ／Ｏインターフェイス内のメモリに記憶する。そして、ホストＣＰＵ８１０は、ボタンが押下されたことの通知を受けると、Ｉ／Ｏインターフェイス内のメモリにアクセスを行い、当該メモリに記憶されたボタンの番号から外部割り込みのタイプを識別し、当該ボタンの番号に対応する割り込みルーチンの実行制御を行う。

このとき、ホストＣＰＵ８１０が、当該ボタンの番号に対応する割り込みルーチンがＳＡＭ１０５$_1$によって実行されるべきものである場合には、ＳＡＭ１０５$_1$に内部割り込みＳ８１０を出してタスク実行を依頼する。

【０１１３】

前述したように、ＳＡＭ１０５$_1$が実行するタスクには、以下に示す①～③などがある。

これらのタスクは、外部割り込み専用線を介してホストＣＰＵ８１０が①～③などに対応する外部割り込みを操作部１６５から受け、ホストＣＰＵ８１０がそ

れに応じた内部割り込みＳ８１０をＳＡＭ１０５$_1$に出すことで、ＳＡＭ１０５$_1$によって実行される。

①．コンテンツ購入処理（鍵の購入処理。試聴含む。）

②．再生処理

③．コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２からのダウンロード（更新処理、利用履歴回収、プログラムダウンロードなど）

【０１１４】

上記①、②では、割り込みを発生させるＩ／Ｏはネットワーク機器１６０$_1$のボタンやＧＵＩなどの外部キーデバイスになる。

上記③は、実際は、コンテンツプロバイダ１０１からプッシュ的にダウンロード用のセキュアコンテナ１０４が送られてくるのではなく、ネットワーク機器１６０$_1$（クライアント）側からポーリングしにいく能動的プル型のため、ダウンロードしたセキュアコンテナ１０４をネットワーク機器１６０$_1$内のダウンロードメモリ１６７に書き込んだ時点で、その状態をホストＣＰＵ８１０は把握している。従って、上記③の場合には、ホストＣＰＵ８１０は、操作部１６５からの外部割り込みＳ１６５を受けることなく、ＳＡＭ１０５$_1$に対して内部割り込みＳ８１０を発生する。

【０１１５】

ＳＡＭ１０５$_1$は、ホストＣＰＵ８１０に対してスレーブのＩ／Ｏデバイスと機能するので、ＳＡＭ１０５$_1$のメインルーチンは電源オンでスタートしてから、その後はスタンバイ（ウェーティング、待ち状態）モードで待機している。

その後、ＳＡＭ１０５$_1$は、マスタであるホストＣＰＵ８１０から内部割り込みＳ８１０を受けた時点で、内部で外部から遮蔽された形で依頼されたタスクを処理し、タスク終了をホストＣＰＵ８１０に外部割り込み（ハードウエア割り込み）で知らせ、ホストＣＰＵ８１０に当該そのタスク結果を拾ってもらう。従って、ＳＡＭ１０５$_1$には、ユーザのメインプログラム（ユーザプログラム）というものがない。

【０１１６】

ＳＡＭ１０５$_1$は、コンテンツの購入処理、再生処理、コンテンツプロバイダ

１０１、並びにＥＭＤサービスセンタ１０２からのダウンロード処理などを割り込みルーチンとして実行する。ＳＡＭ１０５$_1$は、通常は、スタンバイ状態で待機している状態から、ホストＣＰＵ８１０から内部割り込みＳ８１０を受け、その割り込みタイプ（番号）（ファンクションコールのコマンド）に応じた割り込みルーチンを実行し、結果を得た時点で、それをホストＣＰＵ８１０に拾ってもらう。

具体的には、ホストＣＰＵ８１０からＳＡＭ１０５$_1$への内部割り込みＳ８１０によるタスク依頼は、Ｉ／Ｏ命令で行われ、ＳＡＭ１０５$_1$はホストＣＰＵ８１０から受け取ったファンクションコールのコマンドに基づいて自分自身に内部割り込みをかける。ホストＣＰＵ８１０によるＳＡＭ１０５$_1$への内部割り込みは、具体的には、チップセレクト(Chip Select) を行ってＳＡＭ１０５$_1$を選択して行われる。

【０１１７】

上述したように、コンテンツの購入および再生などの外部割り込みＳ１６５をホストＣＰＵ８１０が受けるにも係わらず、それに応じたタスクをＳＡＭ１０５$_1$に依頼して行うのは、それらのタスク内容が鍵の購入処理などに伴う暗号処理、署名生成、署名検証処理などのセキュリティに係わるものだからである。

ＳＡＭ１０５$_1$に格納されている割り込みルーチンは、ホストＣＰＵ８１０のい割り込みルーチンのサブルーチン的な役割をもつ割り込みルーチンといえる。

ホストＣＰＵ８１０によって実行される割り込みルーチンは、ＳＡＭ１０５$_1$の共有メモリ空間に、自らに対して行われた外部割り込みＳ１６５に対応するタスクを依頼する内部割り込み（ファンクションコール）Ｓ８１０を送ることを指示するタスクである。

なお、図２４に示すように、ＳＡＭ１０５$_1$に格納されている割り込みルーチンには、さらにサブルーチンがぶらさがっている。

他の割り込みルーチンに共通なプログラムは、サブルーチンとして定義したほうがコードサイズの節約になり、メモリの節減になるためである。また、ＳＡＭ１０５$_1$の処理は、割り込みルーチンから並列にサブルーチンを定義したり、サブルーチンのさらにサブルーチンを定義するなど、通常のＣＰＵの処理と同様の

手法が採用されている。

【０１１８】

図２３に戻って説明を行う。

前述したように、ホストＣＰＵ８１０は、外部キーデバイスなどのＩ／Ｏからの割り込みを、割り込み専用線による外部割り込み（ハードウエア割り込み）Ｓ１６５として受ける。

各々の外部割り込み専用線には、番号が割り振られていて、その番号に応じてホストＣＰＵ８１０側のシステムメモリに格納されている割り込みベクタテーブルにおいて、相当の割り込みベクタを抜き出して割り込みルーチンを開始する。そのとき、割り込みタイプが、ベクタテーブルの中の割り込みベクタの選択番号を示す間接アクセスと、割り込みタイプが、そのまま割り込みルーチンの開始アドレスを示す直接アクセスの２種類が存在する。

【０１１９】

ホストＣＰＵ８１０は、受けた外部割り込みが、ＳＡＭ１０５$_1$ が行うべきタスクの場合、割り込みルーチンは、ＳＡＭ１０５$_1$ に対して内部割り込みＳ８１０をかけ、ＳＡＭ１０５$_1$ にタスクを実行するように依頼（Ｉ／Ｏ命令）するプログラムである。

タスクの種類はコマンド名で定義されていて、ホストＣＰＵ８１０はＳＡＭ１０５$_1$ に対してコマンドベースの内部割り込みＳ８１０をかける。ＳＡＭ１０５$_1$ は電源オンしたとき、図２４に示すように、初期化プログラムとＳＡＭ内部のIntegrity Check を済ませ、その後はスタンバイ状態で待機するスリープモードとなる。スリープモードでは、ＣＰＵの動作のみを停止させ、すべての割り込みで復帰する。その後、ＳＡＭ１０５$_1$ は、例外処理状態を経てプログラム実行状態に遷移する。その後は、ＳＡＭ１０５$_1$ は、ホストＣＰＵ８１０からのタスク依頼の内部割り込みを受けた時点で相当のタスクを実行して結果を出し、それをホストＣＰＵ８１０に返す。

ホストＣＰＵ８１０は、その結果を受けて次のアクションを行う。但し、ＳＡＭ１０５$_1$ がタスク実行中でも、ホストＣＰＵ８１０は他のタスクを行ってもよい。ホストＣＰＵ８１０は、ＳＡＭ１０５$_1$ によるタスクの実行結果を割り込み

として受けつける。

【０１２０】

ＳＡＭ１０５$_1$が、ホストＣＰＵ８１０から依頼を受けたタスクの実行結果をホストＣＰＵ８１０に知らせる手段としては、ホストＣＰＵ８１０に対し割り込みをかけて、ホストＣＰＵ８１０に当該実行結果を拾ってもらう方法と、ＳＡＭ１０５$_1$の内部のホストＣＰＵ８１０がアクセス可能なアドレス空間上（当該アドレス空間には、ホストＣＰＵ８１０からのリード／ライトコマンド、アドレス情報、データがキャリーされる）にステータスレジスタ（ＳＡＭステータスレジスタと呼ぶ）を設ける方法とがある。後者の方法では、ＳＡＭステータスレジスタ（ＳＡＭ＿ＳＲ）にタスクの種類、タスク待機中、タスク実行中、タスク終了などのフラグを設定できるようにし、当該ＳＡＭステータスレジスタに、ホストＣＰＵ８１０から定期的にポーリング（データの読み込み）を行う。

【０１２１】

第１のＳＡＭステータスレジスタには、ホストＣＰＵ８１０によって読み出される、ＳＡＭ１０５$_1$のステータス（状態）を示すフラグが設定される。

また、第２のＳＡＭステータスレジスタには、ホストＣＰＵ８１０からタスク実行の依頼が出されているか否かのステータスをＳＡＭ１０５$_1$の内部のＣＰＵから読みにいくフラグが設定される。バス調停の優先順位に基づいて、ホストＣＰＵ８１０とＳＡＭ１０５$_1$との双方が、当該第１および第２のＳＡＭステータスレジスタのフラグにアクセスできる。

【０１２２】

具体的には、第１のＳＡＭステータスレジスタには、現在ＳＡＭがタスクを実行中か否か、タスク終了済で結果が得られているか否か、そのときのタスク名は何か、あるいはＳＡＭは現在スタンバイ中でタスク待ちの状態か否かを示すフラグが設けられている。第１のＳＡＭステータスレジスタには、ホストＣＰＵ８１０が定期的にポーリングしにいく。

一方、第２のＳＡＭステータスレジスタには、ホストＣＰＵ８１０からタスク実行の依頼が発生しているか否か、あるいは待機中か否かを示すフラグが設けられている。

ここで、ホストＣＰＵ８１０からは、Ｉ／Ｏ書き込み命令のコマンドがＩ／Ｏデバイスである$SAM105_1$に送られ、続いて、書き込むデータと書き込むアドレス情報が送られる。そのときのアドレス情報（データの格納場所）はホストＣＰＵ８１０と$SAM105_1$との共有メモリ空間内に格納される。

【０１２３】

ここで、$SAM105_1$内のメモリのアドレス空間は、ホストＣＰＵ８１０側からは見えないようにすることが必要なので（耐タンパ性）、ホストＣＰＵ８１０からは、作業スタック用のＳＲＡＭの一部、あるいは外付けのＦｌａｓｈ－ＲＯＭ（ＥＥＰＲＯＭ）の一部しか見えないように、$SAM105_1$内のアドレス空間を管理する回路を構成する。従って、ホストＣＰＵ８１０から、データ量の大きいものは、これらのエリアにデータを書き込んでいくし、データ量の少ないものは$SAM105_1$の内部に、ホストＣＰＵ８１０から見えるように仮設のレジスタを設定して、そこに書き込む。

【０１２４】

割り込みによって実行される割り込みルーチンのアドレスは「割り込みベクタ」と呼ばれる。割り込みベクタは、割り込みタイプの順に割り込みベクタテーブルに格納されている。

【０１２５】

ホストＣＰＵ８１０は、図２５に示すように、外部割り込みを受けると、その割り込みタイプ（番号）にしたがって、メモリに格納された割り込みベクタテーブルから割り込みベクタを取り出し、そのアドレスから始まるルーチンをサブルーチンとして実行する。

本実施形態では、前述した①～③の場合に、対応するＩ／Ｏから物理的な割り込み信号によって外部割り込みが発生し、その割り込みタイプ（番号）にしたがって実行される割り込みルーチンで、Ｉ／Ｏである$SAM105_1$に対して内部割り込み（ソフトウエア割り込み）を利用したファンクションコール（Procedure Call）を行い、自分の代わりに$SAM105_1$にそのタスクの実行を行ってもらい、その結果を受け取って次なるアクションを行う。

内部割り込みは、図２６に示すように、ユーザプログラム中、つまりＣＰＵ内

部から発生するソフトウェア割り込みである。当該内部割り込みは、マシン語のＩＮＴ命令の実行によって発生する。

【０１２６】

以下、ファンクションコール（Procedure Call）について説明する。

割り込みルーチンの中は、さらに細かく機能（ファンクション）に分けられていて、各機能にコマンド名が定義されている。ここで、ユーザプログラムから、割り込み命令ＩＮＴと共にコマンドを指定することで、目的の機能を指定することをファンクションコール（Procedure Call）とよぶ。ファンクションコールは、内部割り込み（ソフトウェア割り込み）を利用したものである。

ファンクションコールでは、ＣＰＵのレジスタにファンクションコール番号を入れて割り込みルーチンに必要なパラメータを渡し、目的の機能（ファンクション）を指定する。その結果はレジスタやメモリに返されるか、あるいは動作となってあらわれる。

例えば、ホストＣＰＵ８１０が図２７に示すユーザプログラム内のコードＡを実行する場合には、「ＩＮＴ　２１Ｈ」によってＣＰＵによって割り込みタイプ「２１Ｈ」の内部割り込みに対応するメモリ内の領域がアクセスされ、コマンド解析部へのアクセスを介して、ファンクション３のサブルーチンが実行される。

【０１２７】

次に、ＳＡＭ１０５$_1$のＣＰＵの処理状態について説明する。

図２８は、ＳＡＭ１０５$_1$のＣＰＵの処理状態を説明するための図である。

図２８に示すように、ＳＡＭ１０５$_1$のＣＰＵの処理状態には、リセット状態ＳＴ１、例外処理状態ＳＴ２、バス権解放状態ＳＴ３、プログラム実行状態ＳＴ４および低消費電力状態ＳＴ５の５種類がある。

以下、各状態について説明する。

リセット状態ＳＴ１：ＣＰＵがリセットされている状態である。

例外処理状態ＳＴ２：リセットや割り込みなどの例外処理要因によってＣＰＵが処理状態の流れを変えるときの過渡的な状態である。割り込みの処理の場合は、ＳＰ（スタックポインタ）を参照してＰＣ（プログラムカウンタ）のカウント値とステータスレジスタ（ＳＲ）の値とをスタック領域に退避する。例外処理ベ

クターテーブルから割り込みルーチンの開始アドレスを取り出し、そのアドレスに分岐してプログラムの実行を開始する。その後の処理状態はプログラム実行状態ＳＴ３となる。

【０１２８】

プログラム実行状態ＳＴ３：ＣＰＵが順次プログラムを実行している状態である。

バス権解放状態ＳＴ４：ＣＰＵがバス権を要求したデバイスにバスを解放する状態である。

【０１２９】

低消費電力状態ＳＴ５：スリープモード、スタンバイモードおよびモジュールスタンバイモードの３つの状態がある。

（１）スリープモード

ＣＰＵの動作は停止するが、ＣＰＵの内部レジスタのデータと、内蔵キャッシュメモリー、および内蔵ＲＡＭのデータは保持される。ＣＰＵ以外の内蔵周辺モジュールの機能は停止しない。

このモードからの復帰は、リセット、すべての割り込み、またはＤＭＡアドレスエラーによって行われ、例外処理状態ＳＴ２を経て通常のプログラム実行状態へ遷移する。

（２）スタンバイモード

スタンバイモードでは、ＣＰＵ、内蔵モジュール、および発振器のすべての機能が停止する。

キャッシュおよび内部ＲＡＭのデータは保持されない。

スタンバイモードからの復帰は、リセット、外部のＮＭＩ割り込みにより行われる。

復帰時は、発振安定時間経過後、例外処理状態を経て通常プログラム状態へ遷移する。

発振器が停止するので、消費電力は著しく低下する。

（３）モジュールスタンバイモード

ＤＭＡなどの内蔵モジュールへのクロック供給を停止することができる。

【０１３０】

次に、ホストＣＰＵ８１０とＳＡＭ１０５$_1$との間の関係をメモリ空間を用いて説明する。

図２９は、ホストＣＰＵ８１０およびＳＡＭ１０５$_1$のメモリ空間を示す図である。

図２９に示すように、ホストＣＰＵ８１０のＣＰＵ８１０ａは、ユーザのボタン操作などに応じた外部割り込みを受けると、ユーザプログラムの実行を中断して、割り込みタイプを指定して割り込みベクタテーブルのハードウェア割り込みの領域にアクセスする。そして、ＣＰＵ８１０ａは、当該アクセスによって得られたアドレスに記憶されている割り込みルーチンを実行する。当該割り込みルーチンは、ＳＡＭに対して内部割り込みであるファンクションコールＣａｌｌ１－１，１－２，２または３を出してＳＡＭに対応するタスクを実行させ、そのタスク実行の結果を得た後に、ユーザプログラムに復帰する処理を記述している。具体的には、ＣＰＵ８１１０ａは、ＳＡＭ１０５$_1$内のメモリ１０５$_1$ａの一部を構成するＳＲＡＭ１１５５に、依頼するタスクを特定する情報を書き込む。ここで、ＳＲＡＭ１１５５は、ホストＣＰＵ８１０とＳＡＭ１０５$_1$との共有メモリである。

【０１３１】

ホストＣＰＵ８１０のＣＰＵ８１０ａは、ＳＡＭ１０５$_1$に内部割り込みを出すときに、ＳＡＭ１０５$_1$内の第２のＳＡＭステータスレジスタ１１５６ｂのタスク待機中のフラグをオンにする。

ＳＡＭ１０５$_1$のＣＰＵ１１００は、第２のＳＡＭステータスレジスタ１１５６ｂを見ると、ＳＲＡＭ１１５５にアクセスして依頼されたタスクの種類を特定し、それに応じた割り込みルーチンを実行する。当該割り込みルーチンは、前述したように、他のサブルーチンを読み出して実行される。当該サブルーチンには、例えば、記録媒体との相互認証、Ａ／Ｖ圧縮・伸長用ＳＡＭとの相互認証、メディア・ドライブＳＡＭとの間の相互認証、ＩＣカードとの間の相互認証、機器間の相互認証、ＥＭＤサービスセンタ１０２との間の相互認証、並びに署名データの生成および検証を行うものがある。

【０１３２】

ＳＡＭ１０５$_1$のＣＰＵ１１００は、当該割り込みルーチンの結果（タスク結果）を、ＳＲＡＭ１１５５内に格納すると共に、ＳＡＭ１０５$_1$内の第１のＳＡＭステータスレジスタ１１５６ａのタスク終了のフラグをオンにする。

そして、ホストＣＰＵ８１０は、第１のＳＡＭステータスレジスタ１１５６ａのタスク終了のフラグがオンにされたことを確認した後に、ＳＲＡＭ１１５５に格納されたタスク結果を読み出し、その後、ユーザプログラムの処理に復帰する。

【０１３３】

以下、ＳＡＭ１０５$_1$の機能を説明する。

ここで、ＳＡＭ１０５$_2$～１０５$_4$の機能は、ＳＡＭ１０５$_1$の機能と同じである。

ＳＡＭ１０５$_1$は、コンテンツ単位の課金処理を行うモジュールであり、ＥＭＤサービスセンタ１０２との間で通信を行う。

ＳＡＭ１０５$_1$は、例えば、ＥＭＤサービスセンタ１０２によって仕様およびバージョンなどが管理され、家庭機器メーカに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカは、ＳＡＭ１０５$_1$のＩＣ(Integrated Circuit)の内部の仕様を知ることはできず、ＥＭＤサービスセンタ１０２が当該ＩＣのインタフェースなどを統一化し、それに従ってネットワーク機器１６０$_1$に搭載される。なお、ＳＡＭ１０５$_2$～１０５$_4$は、それぞれＡＶ機器１６０$_2$～１６０$_4$に搭載される。

【０１３４】

ＳＡＭ１０５$_1$は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Registance) 性を持ったハードウェアモジュール（ＩＣモジュールなど）、あるいはＣＰＵにおいてソフトウェア（秘密プログラム）を実行して実現される機能モジュールである。

ＳＡＭ１０５$_1$の機能をＩＣという形で実現する場合は、ＩＣ内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。ＳＡＭをＩＣという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をＳＡＭとして定義してもよい。

【０１３５】

なお、図２２に示す例では、実線で示されるように、通信モジュール１６２からのセキュアコンテナ１０４をＳＡＭ１０５$_1$に出力する場合を例示するが、点線で示されるように、通信モジュール１６２からＳＡＭ１０５$_1$にキーファイルＫＦを出力し、通信モジュール１６２からダウンロードメモリ１６７にＣＰＵバスなどを介してコンテンツファイルＣＦを直接的にダウンロードメモリ１６７に書き込むようにしてもよい。

また、ＡＶ圧縮・伸長用ＳＡＭ１６３に対してのコンテンツデータＣの出力は、ＳＡＭ１０５$_1$を介して行うのではなく、ダウンロードメモリ１６７から直接的に行うようにしてもよい。

【０１３６】

以下、ＳＡＭ１０５$_1$の機能を機能ブロック図を参照しながら具体的に説明する。

図３０は、ＳＡＭ１０５$_1$の機能の機能ブロック図である。

なお、図３０には、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力し、セキュアコンテナ１０４内のキーファイルＫＦを復号する処理に関連するデータの流れが示されている。

図３０に示すように、ＳＡＭ１０５$_1$は、相互認証部１７０、暗号化・復号部１７１，１７２，１７３、コンテンツプロバイダ管理部１８０、ダウンロードメモリ管理部１８２、ＡＶ圧縮・伸長用ＳＡＭ管理部１８４、ＥＭＤサービスセンタ管理部１８５、利用監視部１８６、課金処理部１８７、署名処理部１８９、ＳＡＭ管理部１９０、メディアＳＡＭ管理部１９７、作業用メモリ２００、外部メモリ管理部８１１およびＣＰＵ１１００を有する。

ＣＰＵ１１００は、ホストＣＰＵ８１０からの内部割り込みＳ８１０を受けて、ＳＡＭ１０５$_1$内の処理を統括的に制御する。

【０１３７】

ここで、コンテンツプロバイダ管理部１８０およびダウンロードメモリ管理部１８２が本発明の入力処理手段に対応し、課金処理部１８７が本発明の決定手段、履歴データ生成手段および利用制御データ生成手段に対応し、暗号化・復号部１７２が本発明の復号手段に対応し、利用監視部１８６が本発明の利用制御手段に対応している。

また、暗号化・復号部１７３が本発明の暗号化手段に対応している。

また、後述する例えば図４５に示すメディア・ドライブＳＡＭ管理部８５５が本発明の記録制御手段に対応している。

また、署名処理部１８９が本発明の署名処理手段に対応している。

【０１３８】

なお、図３０に示すＳＡＭ１０５$_1$の各機能は、前述したように、ＣＰＵにおいて秘密プログラムを実行して実現されるか、あるいは所定のハードウェアによって実現される。ＳＡＭ１０５$_1$のハードウェア構成については後述する。

また、外部メモリ２０１には、以下に示す処理を経て、図３１に示すように、利用履歴データ１０８およびＳＡＭ登録リストが記憶される。

ここで、外部メモリ２０１のメモリ空間は、ＳＡＭ１０５$_1$の外部（例えば、ホストＣＰＵ８１０）からは見ることはできず、ＳＡＭ１０５$_1$のみが外部メモリ２０１の記憶領域に対してのアクセスを管理できる。

外部メモリ２０１としては、例えば、フラッシュメモリあるいは強誘電体メモリ（ＦｅＲＡＭ）などが用いられる。

また、作業用メモリ２００としては、例えばＳＲＡＭが用いられ、図３２に示すように、セキュアコンテナ１０４、コンテンツ鍵データＫｃ、権利書データ（ＵＣＰ）１０６、記憶部１９２のロック鍵データK_{LOC}、コンテンツプロバイダ１０１の公開鍵証明書CER_{CP}、利用制御データ（ＵＣＳ）１６６、およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3などが記憶される。

【０１３９】

以下、ＳＡＭ１０５$_1$の機能のうち、コンテンツプロバイダ１０１からのセキュアコンテナ１０４を入力（ダウンロード）したときの各機能ブロックの処理内

容を図３０を参照しながら説明する。

当該処理は、コンテンツのダウンロードを指示する外部割り込みＳ８１０をホストＣＰＵ８１０から受けたＣＰＵ１１００によって統括的に制御される。

【０１４０】

相互認証部１７０は、ＳＡＭ１０５$_1$ がコンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間でオンラインでデータを送受信する際に、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で相互認証を行ってセッション鍵データ（共有鍵）K_{SES} を生成し、これを暗号化・復号部１７１に出力する。セッション鍵データK_{SES} は、相互認証を行う度に新たに生成される。

【０１４１】

暗号化・復号部１７１は、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２との間で送受信するデータを、相互認証部１７０が生成したセッション鍵データK_{SES} を用いて暗号化・復号する。

【０１４２】

ダウンロードメモリ管理部１８２は、図２２に示すようにダウンロードメモリ１６７が相互認証機能を持つメディアＳＡＭ１６７ａを有している場合には、相互認証部１７０とメディアＳＡＭ１６７ａとの間で相互認証を行った後に、相互認証によって得られたセッション鍵データK_{SES} を用いて暗号化して図２２に示すダウンロードメモリ１６７に書き込む。

ダウンロードメモリ１６７としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。

なお、図３３に示すように、ＨＤＤ(Hard Disk Drive) などの相互認証機能を備えていないメモリをダウンロードメモリ２１１として用いる場合には、ダウンロードメモリ２１１内はセキュアではないので、コンテンツファイルＣＦをダウンロードメモリ２１１にダウンロードし、機密性の高いキーファイルＫＦを例えば、図３０に示す作業用メモリ２００あるいは図２２に示す外部メモリ２０１にダウンロードする。

キーファイルＫＦを外部メモリ２０１に記憶する場合には、例えば、ＳＡＭ１

05_1において、キーファイルＫＦをＣＢＣモードでＭＡＣ鍵データK_{MAC}を用いて暗号化して外部メモリ２０１に記憶し、最後の暗号文ブロックの一部をＭＡＣ(Message Authentication Code)値として$SAM105_1$内に記憶する。そして、外部メモリ２０１から$SAM105_1$にキーファイルＫＦを読み出す場合には、$SAM105_1$内で当該読み出したキーファイルＫＦをＭＡＣ鍵データK_{MAC}を用いて復号し、それによって得たＭＡＣ値と、既に記憶しているＭＡＣ値とを比較することで、キーファイルＫＦが改竄されているか否かを検証する。この場合に、ＭＡＣ値ではなく、ハッシュ値を用いてもよい。

【０１４３】

暗号化・復号部１７２は、ダウンロードメモリ管理部１８２から入力したセキュアコンテナ１０４に格納されたキーファイルＫＦ内のコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3を、記憶部１９２から読み出した対応する期間のライセンス鍵データKD_1～KD_3を用いて復号する。

当該復号されたコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3は、作業用メモリ２００に書き込まれる。

【０１４４】

ＥＭＤサービスセンタ管理部１８５は、図１に示すＥＭＤサービスセンタ１０２との間の通信を管理する。

【０１４５】

署名処理部１８９は、記憶部１９２から読み出したＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$およびコンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を用いて、セキュアコンテナ１０４内の署名データの検証を行なう。

【０１４６】

記憶部１９２は、$SAM105_1$の外部から読み出しおよび書き換えできない秘密データとして、図３４に示すように、有効期限付きの複数のライセンス鍵データKD_1～KD_3、ＳＡＭ＿ＩＤ、ユーザＩＤ、パスワード、当該ＳＡＭが属するホームネットワークグループの識別子ＨＮＧ＿ＩＤ、情報参照用ＩＤ、ＳＡ

M登録リスト、機器および記録媒体のリボケーションリスト、記録用鍵データK_{STR}、ルートＣＡの公開鍵データ$K_{R-CA,P}$、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ドライブ用ＳＡＭの認証用元鍵（共通鍵暗号化方式を採用した場合）、ドライブ用ＳＡの公開鍵証明書（秘密鍵暗号化方式を採用した場合）、$SAM105_1$の秘密鍵データ$K_{SAM1,S}$（共通鍵暗号化方式を採用した場合）、$SAM105_1$の公開鍵データ$K_{SAM1,P}$を格納した公開鍵証明書CER_{SAM1}（秘密鍵暗号化方式を採用した場合）、ＥＭＤサービスセンタ１０２の秘密鍵データ$K_{ESC,S}$を用いた公開鍵証明書CER_{ESC}の署名データSIG_{22}、ＡＶ圧縮・伸長用ＳＡＭ１６３との間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアＳＡＭとの間の相互認証用の元鍵データ（共通鍵暗号化方式を採用した場合）、メディアＳＡＭの公開鍵証明書データCER_{MEDSAM}（公開鍵暗号化方式を採用した場合）、扱える信号の諸元、圧縮方式、接続するモニタ表示能力、フォーマット変換機能、ビットストリームレコーダか有無、権利処理（利益分配）用データ、利益分配する関連エンティティのＩＤなどを記憶している。

なお、図３４において、左側に「＊」を付したデータは、$SAM105_1$の出荷時に記憶部１９２に記憶されており、それ以外のデータは出荷後に行われるユーザ登録時に記憶部１９２に記憶される。

【０１４７】

また、記憶部１９２には、図３０に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。

記憶部１９２としては、例えば、フラッシューＥＥＰＲＯＭ(Electrically Erasable Programmable RAM)が用いられる。

【０１４８】

＜ライセンス鍵データの受信時の処理＞

以下、ＥＭＤサービスセンタ１０２から受信したライセンス鍵データKD_1～KD_3を記憶部１９２に格納する際の$SAM105_1$内での処理の流れを図３３および図３５を参照しながら説明する。

図３５は、ＥＭＤサービスセンタ１０２から受信したライセンス鍵データＫＤ

$_1$～ＫＤ$_3$を記憶部１９２に格納する際のＳＡＭ１０５$_1$内での処理の流れを示すフローチャートである。

ステップＳ３５－０：ＳＡＭ１０５$_1$のＣＰＵ１１００は、ホストＣＰＵ８１０から、ライセンス鍵データの受信処理を行うことを指示する内部割り込みＳ８１０を受ける。

ステップＳ３５－１：ＳＡＭ１０５$_1$の相互認証部１７０と、ＥＭＤサービスセンタ１０２との間で相互認証を行なう。

ステップＳ３５－２：ステップＳ３５－１の相互認証によって得られたセッション鍵データＫ$_{SES}$で暗号化した３カ月分のライセンス鍵データＫＤ$_1$～ＫＤ$_3$およびその署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD3,ESC}$を、ＥＭＤサービスセンタ１０２からＥＭＤサービスセンタ管理部１８５を介して作業用メモリ２００に書き込む。

【０１４９】

ステップＳ３５－３：暗号化・復号部１７１は、セッション鍵データＫ$_{SES}$を用いて、ライセンス鍵データＫＤ$_1$～ＫＤ$_3$およびその署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD3,ESC}$を復号する。

ステップＳ３５－４：署名処理部１８９は、作業用メモリ２００に記憶された署名データＳＩＧ$_{KD1,ESC}$～ＳＩＧ$_{KD3,ESC}$の正当性を確認した後に、ライセンス鍵データＫＤ$_1$～ＫＤ$_3$を記憶部１９２に書き込む。

ステップＳ３５－５：ＣＰＵ１１００は、上述したライセンス鍵データ受信処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述したライセンス鍵データ受信処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０１５０】

＜セキュアコンテナ１０４をコンテンツプロバイダ１０１から入力した時の処理＞

以下、コンテンツプロバイダ１０１が提供したセキュアコンテナ１０４を入力する際のＳＡＭ１０５$_1$内での処理の流れを図３０および図３６を参照しながら

説明する。

なお、以下に示す例では、コンテンツファイルＣＦをＳＡＭ１０５$_1$を介してダウンロードメモリ１６７に書き込む場合を例示するが、本発明は、コンテンツファイルＣＦをＳＡＭ１０５$_1$を介さずに直接的にダウンロードメモリ１６７に書き込むようにしてもよい。

図３６は、ンテンツプロバイダ１０１が提供したセキュアコンテナ１０４を入力する際のＳＡＭ１０５$_1$内での処理の流れを示すフローチャートである。

なお、以下に示す例では、ＳＡＭ１０５$_1$において、セキュアコンテナ１０４を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ１０４の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

ステップＳ３６－０：図３０に示すＳＡＭ１０５$_1$のＣＰＵ１１００は、ホストＣＰＵ８１０から、セキュアコンテナの入力処理を行うことを指示する内部割り込みＳ８１０を受ける。

ステップＳ３６－１：ＳＡＭ１０５$_1$の相互認証部１７０とコンテンツプロバイダ１０１との間で相互認証を行なう。

ステップＳ３６－２：ＳＡＭ１０５$_1$の相互認証部１７０とダウンロードメモリ１６７のメディアＳＡＭ１６７ａとの間で相互認証を行なう。

【０１５１】

ステップＳ３６－３：コンテンツプロバイダ１０１から受信したセキュアコンテナ１０４を、ダウンロードメモリ１６７に書き込む。

このとき、ステップＳ３６－２で得られたセッション鍵データを用いて、相互認証部１７０におけるセキュアコンテナ１０４の暗号化と、メディアＳＡＭ１６７ａにおけるセキュアコンテナ１０４の復号とを行なう。

ステップＳ３６－４：ＳＡＭ１０５$_1$は、ステップＳ３６－１で得られたセッション鍵データを用いて、セキュアコンテナ１０４の復号を行なう。

【０１５２】

ステップＳ３６－５：署名処理部１８９は、図３（Ｃ）に示す署名データ$SIG_{1,ESC}$の検証を行なった後に、図３（Ｃ）に示す公開鍵証明書データCER_{CP}

内に格納されたコンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$を用いて、署名データ$SIG_{6,CP}$，$SIG_{7,CP}$の正当性を検証する。

このとき、署名データ$SIG_{6,CP}$が正当であると検証されたときに、コンテンツファイルＣＦの作成者および送信者の正当性が確認される。

また、署名データ$SIG_{7,CP}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。

【０１５３】

ステップＳ３６－６：署名処理部１８９は、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて、図３（Ｂ）に示すキーファイルＫＦ内の署名データ$SIG_{K1,ESC}$の正当性、すなわちキーファイルＫＦの作成者の正当性およびキーファイルＫＦがＥＭＤサービスセンタ１０２に登録されているか否かの検証を行う。

【０１５４】

ステップＳ３６－７：暗号化・復号部１７２は、記憶部１９２から読み出した対応する期間のライセンス鍵データKD_1～KD_3を用いて、図３（Ｂ）に示すキーファイルＫＦ内のコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3を復号し、これらを作業用メモリ２００に書き込む。

【０１５５】

ステップＳ３６－８：ＣＰＵ１１００は、上述したセキュアコンテナの入力処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述したセキュアコンテナの入力処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０１５６】

以下、ダウンロードメモリ１６７にダウンロードされたコンテンツデータＣを利用・購入する処理に関連する各機能ブロックの処理内容を図３７を参照しながら説明する。

以下に示す各機能ブロックの処理は、ホストＣＰＵ８１０からの内部割り込み

Ｓ８１０を受けたＣＰＵ１１００によって統括的に制御される。

【０１５７】

利用監視部１８６は、作業用メモリ２００から権利書データ１０６および利用制御データ１６６を読み出し、当該読み出した権利書データ１０６および利用制御データ１６６によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。

ここで、権利書データ１０６は、図３６を用いて説明したように、復号後に作業用メモリ２００に記憶されたキーファイルＫＦ内に格納されている。

また、利用制御データ１６６は、後述するように、ユーザによって購入形態が決定されたときに、作業用メモリ２００に記憶される。

なお、利用制御データ１６６には、当該コンテンツデータＣを購入したユーザのユーザＩＤおよびトレーシング(Tracing) 情報が記述され、取扱制御情報として購入形態決定処理で決定された購入形態が記述されている点を除いて、図３に示す権利書データ１０６と同じデータが記述されている。

【０１５８】

課金処理部１８７は、図２２に示すホストＣＰＵ８１０からコンテンツの購入あるいは利用の形態を決定することを指示する内部割り込みＳ８１０を受けたときに、それに応じた利用履歴データ１０８を作成する。

ここで、利用履歴データ１０８は、前述したように、ユーザによるセキュアコンテナ１０４の購入および利用の形態の履歴を記述しており、ＥＭＤサービスセンタ１０２において、セキュアコンテナ１０４の購入に応じた決済処理およびライインセンス料の支払いを決定する際に用いられる。

【０１５９】

また、課金処理部１８７は、必要に応じて、作業用メモリ２００から読み出した販売価格あるいは標準小売価格データＳＲＰをユーザに通知する。

ここで、販売価格および標準小売価格データＳＲＰは、復号後に作業用メモリ２００に記憶された図３（Ｂ）に示すキーファイルＫＦの権利書データ１０６内に格納されている。

課金処理部１８７による課金処理は、利用監視部１８６の監視の下、権利書デ

ータ１０６が示す使用許諾条件などの権利内容および利用制御データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【０１６０】

また、課金処理部１８７は、外部割り込みＳ８１０に基づいて、ユーザによって決定されたコンテンツの購入形態を記述した利用制御（UCS: Usage Control Status)データ１６６を生成し、これを作業用メモリ２００に書き込む。

本実施形態では、購入形態を決定した後に、利用制御データ１６６を作業用メモリ２００に記憶する場合を例示したが、利用制御データ１６６およびコンテンツ鍵データＫｃを外付けメモリである外部メモリ２０１に格納するようにしてもよい。外部メモリ２０１としは、前述したように、例えばＮＶＲＡＭであるフラッシュメモリが用いられる。外部メモリ２０１に書き込みを行う場合には外部メモリ２０１の正当性の検証であるインテグリティチェック(Integrity Check) を行うが、この際に外部メモリ２０１の記憶領域を複数のブロックに分け、ブロック毎にＳＨＡ－１あるいはＭＡＣなどでハッシュ値を求め、当該ハッシュ値をＳＡＭ１０５$_1$ 内で管理する。

なお、ＳＡＭ１０５$_1$ において、購入形態を決定せずに、セキュアコンテナ１０４を他のＳＡＭ１０５$_2$ ～１０５$_4$ に転送してもよい。この場合には、利用制御データ１６６は作成されない。

【０１６１】

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切り(Sell Through)、利用期間に制限を持たせるタイムリミテッド(Time Limited)、再生する度に課金を行なう再生課金(Pay Per Play)、ＳＣＭＳ機器を用いた複製において再生する度に課金を行なう再生課金(Pay Per SCMS)、ＳＣＭＳ機器において複製を認める(Sell Through SCMS Copy)、および複製のガードを行わずに再生する度に課金を行う再生課金(Pay Per Copy N without copy guard) などがある。

ここで、利用制御データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが

当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ１６６には、コンテンツのＩＤ、購入形態、当該購入形態に応じた価格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ＿ＩＤ，購入を行なったユーザのＵＳＥＲ＿ＩＤなどが記述されている。

【０１６２】

なお、決定された購入形態が再生課金である場合には、例えば、ＳＡＭ１０５$_1$からコンテンツプロバイダ１０１に利用制御データ１６６をコンテンツデータＣの購入と同時にリアルタイムに送信し、コンテンツプロバイダ１０１がＥＭＤサービスセンタ１０２に、利用履歴データ１０８を所定の期間内にＳＡＭ１０５$_1$に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御データ１６６が、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御データ１６６をコンテンツプロバイダ１０１にリアルタイムに送信する。

【０１６３】

ＥＭＤサービスセンタ管理部１８５は、所定の期間毎に、外部メモリ管理部８１１を介して外部メモリ２０１から読み出した利用履歴データ１０８をＥＭＤサービスセンタ１０２に送信する。

このとき、ＥＭＤサービスセンタ管理部１８５は、署名処理部１８９において、秘密鍵データ$K_{SAM1,s}$を用いて利用履歴データ１０８の署名データ$SIG_{200,SAM1}$を作成し、署名データ$SIG_{200,SAM1}$を利用履歴データ１０８と共にＥＭＤサービスセンタ１０２に送信する。

ＥＭＤサービスセンタ１０２への利用履歴データ１０８の送信は、例えば、ＥＭＤサービスセンタ１０２からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ１０８に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ２０１の記憶容量に応じて決定される。

【０１６４】

ダウンロードメモリ管理部１８２は、例えば、図２２に示すホストＣＰＵ８１０からコンテンツの再生動作を行う旨の内部割り込みＳ８１０をＣＰＵ１１００が受けた場合に、ダウンロードメモリ１６７から読み出したコンテンツデータＣ、作業用メモリ２００から読み出したコンテンツ鍵データＫｃおよび課金処理部１８７から入力したユーザ電子透かし情報用データ１９６をＡＶ圧縮・伸長用ＳＡＭ管理部１８４に出力する。

また、ＡＶ圧縮・伸長用ＳＡＭ管理部１８４は、ホストＣＰＵ８１０からの外部割り込みＳ１６５に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ１６７から読み出したコンテンツファイルＣＦ、並びに作業用メモリ２００から読み出したコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９をＡＶ圧縮・伸長用ＳＡＭ管理部１８４に出力する。

【０１６５】

ここで、半開示パラメータデータ１９９は、権利書データ１０６内に記述されており、試聴モード時のコンテンツの取り扱いを示している。ＡＶ圧縮・伸長用ＳＡＭ１６３では、半開示パラメータデータ１９９に基づいて、暗号化されたコンテンツデータＣを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、ＡＶ圧縮・伸長用ＳＡＭ１６３がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ１９９によって、コンテンツ鍵データＫｃを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【０１６６】

＜ダウンロードしたセキュアコンテナの購入形態決定処理＞

以下、コンテンツプロバイダ１０１からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ１０４の購入形態を決定するまでのＳＡＭ105_1の処理の流れを図３７および図３８を参照しながら説明する。

なお、以下に示す処理では、セキュアコンテナ１０４の購入形態を決定する際に、セキュアコンテナ１０４内の各データの署名データの検証を行わない（前述

したようにセキュアコンテナ１０４の受信時に署名データの検証を行う）場合を例示するが、当該購入形態を決定する際にこれらの署名データの検証を行ってもよい。

図３８は、コンテンツプロバイダ１０１からダウンロードメモリ１６７にダウンロードされたセキュアコンテナ１０４の購入形態を決定するまでの処理の流れを示すフローチャートである。

ステップＳ３８－０：図３７に示すＳＡＭ１０５$_1$のＣＰＵ１１００は、ホストＣＰＵ８１０から、コンテンツの購入形態を決定することを指示する内部割り込みＳ８１０を受ける。

【０１６７】

ステップＳ３８－１：ＣＰＵ１１００は、ホストＣＰＵ８１０からの内部割り込みＳ８１０が試聴モードを指定しているか否かを判断し、指定されたと判断した場合にはステップＳ３８－２の処理を実行し、出力されていないと判断した場合にはステップＳ３８－５の処理を実行する。

【０１６８】

ステップＳ３８－２：作業用メモリ２００から読み出されたコンテンツ鍵データＫｃおよび半開示パラメータデータ１９９が、図３２に示すＡＶ圧縮・伸長用ＳＡＭ１６３に出力される。このとき、相互認証部１７０と相互認証部２２０との間の相互認証後に、コンテンツ鍵データＫｃおよび半開示パラメータデータ１９９に対してセッション鍵データK_{SES}による暗号化および復号が行なわれる。

【０１６９】

ステップＳ３８－３：ＣＰＵ１１００は、ホストＣＰＵ８１０から試聴モードを行うことを示す内部割り込みＳ８１０を受けると、例えば、ダウンロードメモリ１６７に記憶されているコンテンツファイルＣＦが、ＡＶ圧縮・伸長用ＳＡＭ管理部１８４を介して、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３に出力される。

このとき、コンテンツファイルＣＦに対して、相互認証部１７０とメディアＳＡＭ１６７ａとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部１７０と相互認証部２２０との間の相互認証およびセッショ

ン鍵データK_{SES}による暗号化・復号とが行なわれる。

コンテンツファイルＣＦは、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３の復号部２２１においてセッション鍵データK_{SES}を用いて復号された後に、復号部２２２に出力される。

【０１７０】

ステップＳ３８－４：復号された半開示パラメータデータ１９９が半開示処理部２２５に出力され、半開示処理部２２５からの制御によって、復号部２２２によるコンテンツ鍵データＫｃを用いたコンテンツデータＣの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータＣが、伸長部２２３において伸長された後に、電子透かし情報処理部２２４に出力される。

次に、電子透かし情報処理部２２４においてコンテンツデータＣにユーザ電子透かし情報用データ１９６が埋め込まれ、コンテンツデータＣが再生モジュール１６９において再生され、コンテンツデータＣに応じた音響が出力される。

また、電子透かし情報処理部２２４では、コンテンツデータＣに埋め込まれている電子透かし情報が検出され、当該検出の結果に基づいて、処理の停止の有無を決定する。

【０１７１】

ステップＳ３８－５：ユーザが操作部１６５を操作して購入形態を決定すると、当該決定に応じた内部割り込みＳ８１０がホストＣＰＵ８１０からＳＡＭ１０$5_1$に出される。

ステップＳ３８－６：ＳＡＭ１０$5_1$の課金処理部１８７において、決定された購入形態に応じた利用履歴データ１０８および利用制御データ１６６が生成され、利用履歴データ１０８が外部メモリ管理部８１１を介して外部メモリ２０１に書き込まれると共に、利用制御データ１６６が作業用メモリ２００に書き込まれる。

以後は、利用監視部１８６において、利用制御データ１６６によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

【０１７２】

ステップＳ３８－７：後述する図３９（Ｃ）に示す新たなキーファイルKF_1が作成され、当該作成されたキーファイルKF_1がダウンロードメモリ管理部１８２を介してダウンロードメモリ１６７あるいはその他のメモリに記憶される。

図３９（Ｃ）に示すように、キーファイルKF_1に格納された利用制御データ１６６はストレージ鍵データK_{STR}およびメディア鍵データK_{MED}を用いてＤＥＳのＣＢＣモードを利用して順に暗号化されている。

ここで、記録用鍵データK_{STR}は、例えばＳＡＣＤ(Super Audio Compact Disc)、ＤＶＤ(Digital Versatile Disc)機器、ＣＤ－Ｒ機器およびＭＤ(Mini Disc)機器などの種類に応じて決まるデータであり、機器の種類と記録媒体の種類とを１対１で対応づけるために用いられる。また、メディア鍵データK_{MED}は、記録媒体にユニークなデータである。

【０１７３】

ステップＳ３８－８：署名処理部１８９において、$SAM105_1$の秘密鍵データ$K_{SAM1,S}$を用いて、キーファイルKF_1のハッシュ値H_{K1}が作成され、当該作成されたハッシュ値H_{K1}が、キーファイルKF_1と対応付けられて作業用メモリ２００に書き込まれる。ハッシュ値H_{K1}は、キーファイルKF_1の作成者の正当性およびキーファイルKF_1が改竄されたか否かを検証するために用いられる。

なお、購入形態が決定されたコンテンツデータＣを、例えば、記録媒体に記録したり、オンラインを介して送信する場合には、図３９に示すように、キーファイルKF_1およびハッシュ値H_{K1}、コンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$、キーファイルＫＦおよびその署名データ$SIG_{7,CP}$、公開鍵証明書データCER_{cp}およびその署名データ$SIG_{1,ESC}$、公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$を格納したセキュアコンテナ１０４ｐが作成される。

上述したようにセキュアコンテナ１０４の購入形態を決定すると、利用制御データ１６６が生成されて作業用メモリ２００に記憶されるが、$SAM105_1$において再び同じセキュアコンテナ１０４について購入形態を再決定する場合には

、操作信号Ｓ１６５に応じて作業用メモリ２００に記憶されている利用制御データ１６６が更新される。

【０１７４】

ステップＳ３８－９：ＣＰＵ１１００は、上述したコンテンツの購入形態決定処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述したコンテンツの購入形態決定処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０１７５】

＜コンテンツデータの再生処理＞

次に、ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣを再生する場合の処理の流れを、図４０を参照しながら説明する。

図４０は、当該処理を示すフローチャートである。

当該処理を行う前提として、前述した購入形態の決定処理によって作業用メモリ２００に、利用制御データ１６６が格納されている。

ステップＳ４０－０：図３７に示すＳＡＭ105_1のＣＰＵ１１００は、ホストＣＰＵ８１０から、コンテンツの再生処理を行うことを指示する内部割り込みＳ８１０を受ける。

【０１７６】

ステップＳ４０－１：作業用メモリ２００から利用監視部１８６に、利用制御データ１６６が読み出され、利用制御データ１６６が示す再生条件が解釈・検証され、その結果に基づいて以後の再生処理が行われるように監視される。

ステップＳ４０－２：図３７に示す相互認証部１７０と、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３の相互認証部２２０との間で相互に認証が行われ、セッション鍵データK_{SES}が共有される。

【０１７７】

ステップＳ４０－３：ステップＳ４０－１で解釈・検証された再生条件と、作

業用メモリ２００から読み出されたコンテンツ鍵データＫｃとが、ステップＳ４０－２で得られたセッション鍵データK_{SES}を用いて暗号化された後に、ＡＶ圧縮・伸長用ＳＡＭ１６３に出力される。

これによって、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３の復号部２２１においてセッション鍵データK_{SES}を用いて再生条件およびコンテンツ鍵データＫｃが復号される。

【０１７８】

ステップＳ４０－４：ダウンロードメモリ１６７から読み出されたコンテンツファイルＣＦが、ステップＳ４０－２で得られたセッション鍵データK_{SES}を用いて暗号化された後に、ＡＶ圧縮・伸長用ＳＡＭ１６３に出力される。

これによって、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３の復号部２２１においてセッション鍵データK_{SES}を用いてコンテンツファイルＣＦが復号される。　続いて、ＡＶ圧縮・伸長用ＳＡＭ１６３の伸長部２２３において、コンテンツファイルＣＦ内のコンテンツデータＣが伸長され、電子透かし情報処理部２２４においてユーザ電子透かし情報を埋め込んだ後に再生モジュール１６９において再生される。

【０１７９】

ステップＳ４０－５：必要に応じて、ステップＳ４０－１で読み出された利用制御データ１６６が更新され、再び作業用メモリ２００に書き込まれる。

また、外部メモリ２０１に記憶されている利用履歴データ１０８が更新あるいは作成される。

【０１８０】

ステップＳ４０－６：ＣＰＵ１１００は、上述したコンテンツの再生処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述したコンテンツの再生処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０１８１】

＜一の機器の利用制御データ（ＵＳＣ）１６６を使用して他の機器で再購入を

行う場合の処理＞

先ず、図４１に示すように、例えば、ネットワーク機器１６０$_1$のダウンロードメモリ１６７にダウンロードされたコンテンツファイルＣＦの購入形態を前述したように決定した後に、当該コンテンツファイルＣＦを格納した新たなセキュアコンテナ１０４ｘを生成し、バス１９１を介して、ＡＶ機器１６０$_2$のＳＡＭ１０５$_2$にセキュアコンテナ１０４ｘを転送するまでのＳＡＭ１０５$_1$内での処理の流れを図４２および図４３を参照しながら説明する。

【０１８２】

図４３は、当該処理のフローチャートである。

図４３に示す処理を行う前提として、前述した購入処理によって、ＳＡＭ１０５$_1$の作業用メモリ２００には図４４（Ｃ）に示すキーファイルＫＦ$_1$およびハッシュ値H_{K1}が記憶されている。

ステップＳ４３－１：ユーザによる操作部１６５の操作に応じて、購入形態を既に決定したセキュアコンテナをＳＡＭ１０５$_2$に転送することを示す内部割り込みＳ８１０を、図４２に示すＣＰＵ１１００が受ける。

それに応じて、課金処理部１８７は、外部メモリ２０１に記憶されている利用履歴データ１０８を更新する。

【０１８３】

ステップＳ４３－２：ＳＡＭ１０５$_1$は、後述するＳＡＭ登録リストを検証し、セキュアコンテナの転送先のＳＡＭ１０５$_2$が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ４３－３以降の処理を行う。

また、ＳＡＭ１０５$_1$は、ＳＡＭ１０５$_2$がホームネットワーク内のＳＡＭであるか否かの検証も行う。

【０１８４】

ステップＳ４３－３：相互認証部１７０は、ＳＡＭ１０５$_2$との間で相互認証を行って得たセッション鍵データK_{SES}を共用する。

【０１８５】

ステップＳ４３－４：ＳＡＭ管理部１９０は、ダウンロードメモリ２１１から

図３９（Ａ）に示すコンテンツファイルＣＦおよび署名データ$ＳＩＧ_{6,CP}$を読み出し、これについてのＳＡＭ１０５$_1$の秘密鍵データ$Ｋ_{SAM1}$を用いた署名データ$ＳＩＧ_{41,SAM1}$を署名処理部１８９に作成させる。

【０１８６】

ステップＳ４３－５：ＳＡＭ管理部１９０は、ダウンロードメモリ２１１から図３９（Ｂ）に示すキーファイルＫＦおよび署名データ$ＳＩＧ_{7,CP}$を読み出し、これについてのＳＡＭ１０５$_1$の秘密鍵データ$Ｋ_{SAM1}$を用いた署名データ$ＳＩＧ_{42,SAM1}$を署名処理部１８９に作成させる。

【０１８７】

ステップＳ４３－６：ＳＡＭ管理部１９０は、図４４に示すセキュアコンテナ１０４ｘを作成する。

ステップＳ４３－７：暗号化・復号部１７１において、ステップＳ４３－３で得たセッション鍵データ$Ｋ_{SES}$を用いて、図４４に示すセキュアコンテナ１０４ｘが暗号化される。

【０１８８】

ステップＳ４３－８：ＳＡＭ管理部１９０は、セキュアコンテナ１０４ｘを図４１に示すＡＶ機器１６０$_2$のＳＡＭ１０５$_2$に出力する。

このとき、ＳＡＭ１０５$_1$とＳＡＭ１０５$_2$との間の相互認証と並行して、ＩＥＥＥ１３９４シリアルバスであるバス１９１の相互認証が行われる。

【０１８９】

ステップＳ４３－９：ＣＰＵ１１００は、上述した購入形態を既に決定したセキュアコンテナをＳＡＭ１０５$_2$に転送する処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述した購入形態を既に決定したセキュアコンテナをＳＡＭ１０５$_2$に転送する処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０１９０】

以下、図４１に示すように、ＳＡＭ１０５$_1$から入力した図４４に示すセキュ

アコンテナ１０４ｘを、ＲＡＭ型などの記録媒体（メディア）１３０$_4$に書き込む際のＳＡＭ１０５$_2$内での処理の流れを図４５、図４６および図４７を参照して説明する。

図４６および図４７は、当該処理を示すフローチャートである。

ここで、ＲＡＭ型の記録媒体１３０$_4$は、例えば、セキュアでないＲＡＭ領域１３４、メディアＳＡＭ１３３およびセキュアＲＡＭ領域１３２を有している。

ステップＳ４６－０：図４５に示すＣＰＵ１１００は、図４１に示すＡＶ機器１６０$_2$のホストＣＰＵ８１０から、ネットワーク機器１６０$_1$からのセキュアコンテナを入力することを示す内部割り込みＳ８１０を受ける。

【０１９１】

ステップＳ４６－１：ＳＡＭ１０５$_2$は、ＳＡＭ登録リストを検証し、セキュアコンテナの転送元のＳＡＭ１０５$_1$が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ４６－２以降の処理を行う。

また、ＳＡＭ１０５$_2$は、ＳＡＭ１０５$_1$がホームネットワーク内のＳＡＭであるか否かの検証も行う。

【０１９２】

ステップＳ４６－２：前述したステップＳ４３－２に対応する処理として、ＳＡＭ１０５$_2$は、ＳＡＭ１０５$_1$との間で相互認証を行って得たセッション鍵データK_{SES}を共用する。

ステップＳ４６－３：ＳＡＭ１０５$_2$のＳＡＭ管理部１９０は、図４１および図４５に示すように、ネットワーク機器１６０$_1$のＳＡＭ１０５$_1$からセキュアコンテナ１０４ｘを入力する。

ステップＳ４６－４：暗号化・復号部１７１は、ステップＳ４６－２で共用したセッション鍵データK_{SES}を用いて、ＳＡＭ管理部１９０を介して入力したセキュアコンテナ１０４ｘを復号する。

【０１９３】

ステップＳ４６－５：セッション鍵データK_{SES}を用いて復号されたセキュアコンテナ１０４ｘ内のコンテンツファイルＣＦが、図３９に示すメディア・ドラ

ブＳＡＭ２６０におけるセクタライズ(Sectorize)、セクタヘッダの付加処理、スクランブル処理、ＥＣＣエンコード処理、変調処理および同期処理を経て、ＲＡＭ型の記録媒体１３０$_4$のＲＡＭ領域１３４に記録される。

【０１９４】

ステップＳ４６－６：セッション鍵データK_{SES}を用いて復号されたセキュアコンテナ１０４ｘ内の署名データ$SIG_{6,CP}$，$SIG_{41,SAM1}$と、キーファイルＫＦおよびその署名データ$SIG_{7,CP}$，$SIG_{42,SAM1}$と、キーファイルKF_1およびそのハッシュ値H_{K1}と、公開鍵署名データCER_{CP}およびその署名データ$SIG_{1,ESC}$と、公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とが、作業用メモリ２００に書き込まれる。

【０１９５】

ステップＳ４６－７：署名処理部１８９において、記憶部１９２から読み出した公開鍵データ$K_{CP,P}$を用いて、公開鍵証明書データCER_{CP}，CER_{SAM1}の正当性が確認される。

そして、署名処理部１８９において、公開鍵証明書データCER_{SAM1}に格納された公開鍵データ$K_{CP,P}$を用いて、署名データ$SIG_{6,CP}$の正当性が検証され、コンテンツファイルＣＦの作成者の正当性が確認される。また、署名処理部１８９において、公開鍵証明書データCER_{SAM1}に格納された公開鍵データ$K_{SAM1,P}$を用いて、署名データ$SIG_{41,SAM1}$の正当性が検証され、コンテンツファイルＣＦの送信者の正当性が確認される。

【０１９６】

ステップＳ４６－８：署名処理部１８９は、公開鍵データK_{CP}，$K_{SAM1,P}$を用いて、作業用メモリ２００に記憶されている署名データ$SIG_{7,CP}$，$SIG_{42,SAM1}$の正当性を検証する。そして、署名データ$SIG_{7,CP}$，$SIG_{42,SAM1}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。

【０１９７】

ステップＳ４６－９：署名処理部１８９は、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて、図４４（Ｂ）に示すキーファイルＫＦに格納された

署名データＳＩＧ$_{K1,ESC}$の正当性を確認する。

そして、署名データＳＩＧ$_{K1,ESC}$が正当であると検証されたときに、キーファイルＫＦの作成者の正当性が確認される。

【０１９８】

ステップＳ４６－１０：署名処理部１８９は、ハッシュ値Ｈ$_{K1}$の正当性を検証し、キーファイルＫＦ$_1$の作成者および送信者の正当性を確認する。

なお、当該例では、キーファイルＫＦ$_1$の作成者と送信元とが同じ場合を述べたが、キーファイルＫＦ$_1$の作成者と送信元とが異なる場合には、キーファイルＫＦ$_1$に対して作成者の署名データと送信者と署名データとが作成され、署名処理部１８９において、双方の署名データの正当性が検証される。

【０１９９】

ステップＳ４６－１１：利用監視部１８６は、ステップＳ４６－１０で復号されたキーファイルＫＦ$_1$に格納された利用制御データ１６６を用いて、以後のコンテンツデータＣの購入・利用形態を制御する。

【０２００】

ステップＳ４６－１２：ユーザが操作部１６５を操作して購入形態を決定すると、それに応じた内部割り込みＳ８１０をＳＡＭ１０５$_2$のＣＰＵ１１００が受ける。

ステップＳ４６－１３：課金処理部１８７は、ＣＰＵ１１００からの制御に基づいて、外部メモリ２０１に記憶されている利用履歴データ１０８を更新する。

また、課金処理部１８７は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ１６６を更新する。

このとき送信元のＳＡＭの利用制御データ１６６は破棄される。

【０２０１】

ステップＳ４６－１４：暗号化・復号部１７３は、記憶部１９２から読み出した記録用鍵データＫ$_{STR}$、メディア鍵データＫ$_{MED}$および購入者鍵データＫ$_{PIN}$を順に用いて、ステップＳ４６－１２で生成された利用制御データ１６６を暗号化してメディア・ドライブＳＡＭ管理部８５５に出力する。

ステップＳ４６－１５：メディア・ドライブＳＡＭ管理部８５５は、新たな利

用制御データ１６６を格納したキーファイルKF_1を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ＥＣＣエンコード処理、変調処理および同期処理を経て、ＲＡＭ型の記録媒体130_4のセキュアＲＡＭ領域１３２に記録する。

なお、メディア鍵データK_{MED}は、図４５に示す相互認証部１７０と図４１に示すＲＡＭ型の記録媒体130_4のメディアＳＡＭ１３３との間の相互認証によって記憶部１９２に事前に記憶されている。

【０２０２】

ここで、記録用鍵データK_{STR}は、例えばＳＡＣＤ(Super Audio Compact Disc)、ＤＶＤ(Digital Versatile Disc)機器、ＣＤ－Ｒ機器およびＭＤ(Mini Disc)機器などの種類（当該例では、ＡＶ機器160_2）に応じて決まるデータであり、機器の種類と記録媒体の種類とを１対１で対応づけるために用いられる。なお、ＳＡＣＤとＤＶＤとでは、ディスク媒体の物理的な構造が同じであるため、ＤＶＤ機器を用いてＳＡＣＤの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データK_{STR}は、このような場合において、不正コピーを防止する役割を果たす。

なお、本実施形態では、記録用鍵データK_{STR}を用いた暗号化を行わないようにしてもよい。

【０２０３】

また、メディア鍵データK_{MED}は、記録媒体（当該例では、ＲＡＭ型の記録媒体130_4）にユニークなデータである。

メディア鍵データK_{MED}は、記録媒体（当該例では、図４１に示すＲＡＭ型の記録媒体130_4）側に格納されており、記録媒体のメディアＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データK_{MED}は、記録媒体にメディアＳＡＭが搭載されている場合には、当該メディアＳＡＭ内に記憶されており、記録媒体にメディアＳＡＭが搭載されていない場合には、例えば、ＲＡＭ領域内の図示しないホストＣＰＵの管理外の領域に記憶されている。

なお、本実施形態のように、機器側のＳＡＭ（当該例では、$SAM105_2$）

とメディアＳＡＭ（当該例では、メディアＳＡＭ１３３）との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データK_{MED}を機器側のＳＡＭに転送し、機器側のＳＡＭにおいてメディア鍵データK_{MED}を用いた暗号化および復号を行なってもよい。

本実施形態では、記録用鍵データK_{STR}およびメディア鍵データK_{MED}が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【０２０４】

また、購入者鍵データK_{PIN}は、コンテンツファイルＣＦの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してＥＭＤサービスセンタ１０２によって割り当てられる。購入者鍵データK_{PIN}は、ＥＭＤサービスセンタ１０２において管理される。

【０２０５】

ステップＳ４６－１６：キーファイルＫＦが作業用メモリ２００から読み出され、メディア・ドライブＳＡＭ管理部８５５を介して、図４１に示すメディア・ドラブＳＡＭ２６０によってＲＡＭ型の記録媒体130_4のセキュアＲＡＭ領域１３２に書き込まれる。

【０２０６】

ステップＳ４６－１７：$SAM105_2$のＣＰＵ１１００は、上述したセキュアコンテナの入力処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述したセキュアコンテナの入力処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０２０７】

また、上述した実施形態では、メディア・ドラブＳＡＭ２６０による処理を経て、キーファイルＫＦ，KF_1をＲＡＭ型の記録媒体130_4のセキュアＲＡＭ領域１３２に記録する場合を例示したが、図４１において点線で示すように、$SAM105_2$からメディアＳＡＭ１３３にキーファイルＫＦ，KF_1を記録するようにしてもよい。

【０２０８】

また、上述した実施形態では、ＳＡＭ１０５$_1$からＳＡＭ１０５$_2$にセキュアコンテナ１０４ｘを送信する場合を例示したが、ネットワーク機器１６０$_1$のホストＣＰＵおよびＡＶ機器１６０$_2$のホストＣＰＵによって、コンテンツファイルＣＦおよび権利書データ１０６をネットワーク機器１６０$_1$からＡＶ機器１６０$_2$に送信してもよい。この場合には、ＳＡＭ１０５$_1$からＳＡＭ１０５$_2$に、利用制御データ１６６およびコンテンツ鍵データＫｃが送信される。

【０２０９】

また、その他の実施形態として、例えば、ＳＡＭ１０５$_1$において購入形態を決定し、ＳＡＭ１０５$_2$では購入形態を決定せずに、ＳＡＭ１０５$_1$において生成した利用制御データ１６６をＳＡＭ１０５$_2$でそのまま用いてもよい。この場合には、利用履歴データ１０８は、ＳＡＭ１０５$_1$において生成され、ＳＡＭ１０５$_2$では生成されない。

また、コンテンツデータＣの購入は、例えば、複数のコンテンツデータＣからなるアルバムを購入する形態で行ってもよい。この場合に、アルバムを構成する複数のコンテンツデータＣは、異なるコンテンツプロバイダ１０１によって提供されてもよい（後述する第２実施形態の場合には、さらに異なるサービスプロバイダ３１０によって提供されてもよい）。また、アルバムを構成する一部のコンテンツデータＣについての購入を行った後に、その他のコンテンツデータＣを追加する形で購入を行い、最終的にアルバムを構成する全てのコンテンツデータＣを購入してもよい。

【０２１０】

図４８は、コンテンツデータＣの種々の購入形態の例を説明するための図である。

図４８に示すように、ＡＶ機器１６０$_3$は、ネットワーク機器１６０$_1$がコンテンツプロバイダ１０１から受信したコンテンツデータＣを、権利書データ１０６を用いて購入し、利用制御データ１６６ａを生成している。

また、ＡＶ機器１６０$_2$は、ネットワーク機器１６０$_1$がコンテンツプロバイダ１０１から受信したコンテンツデータＣを、権利書データ１０６を用いて購入

し、利用制御データ１６６ｂを生成している。

また、ＡＶ機器160_3は、ＡＶ機器160_2が購入したコンテンツデータＣを複製し、ＡＶ機器160_2で作成した利用制御データ１６６ｂを用いて利用形態を決定している。これにより、ＡＶ機器160_3において、利用制御データ１６６ｃが作成される。また、ＡＶ機器160_3では、利用制御データ１６６ｃから利用履歴データ１０８ｂが作成される。

また、ＡＶ機器160_4は、ネットワーク機器160_1がコンテンツプロバイダ１０１から受信して購入形態を決定したコンテンツデータＣを入力し、ネットワーク機器160_1が作成した利用制御データ１６６を用いて当該コンテンツデータＣの購入形態を決定する。これにより、ＡＶ機器160_4において、利用制御データ１６６ａが作成される。また、ＡＶ機器160_4では、利用制御データ１６６ａから利用履歴データ１０８ａが作成される。

なお、利用制御データ１６６ａ，１６６ｂ，１６６ｃは、ＡＶ機器160_4，160_2，160_3において、それぞれ固有の記録用鍵データS_{STR}、並びに記録メディア（媒体）に固有のメディア鍵データK_{MED}を用いて暗号化され、記録媒体に記録される。

本実施形態では、ユーザは、コンテンツデータＣの所有権に対して対価を支払うのではなく、使用権に対価を支払う。コンテンツデータの複製は、コンテンツのプロモーションに相当し、マーケットの拡販という観点からコンテンツデータの権利者の要請にかなう行為となる。

【０２１１】

＜ＲＯＭ型の記録媒体のコンテンツデータの購入形態決定処理＞

図４９に示すように、コンテンツの購入形態が未決定の図１１に示すＲＯＭ型の記録媒体130_1をユーザホームネットワーク３０３がオフラインで配給を受けた場合に、ＡＶ機器160_2において購入形態を決定する際の処理の流れを図５０および図５１を参照しながら説明する。

図５１は、当該処理のフローチャートである。

ステップＳ５１－０：ユーザによる操作部１６５の操作に応じて、ＲＯＭ型の記録媒体を用いて配給されたコンテツの購入形態を決定することを示す内部割り

込みＳ８１０を、図５０に示すＳＡＭ１０５$_2$のＣＰＵ１１００が受ける。

ステップＳ５１－１：ＳＡＭ１０５$_2$は、図５０に示す相互認証部１７０と図１１に示すＲＯＭ型の記録媒体１３０$_1$のメディアＳＡＭ１３３との間で相互認証を行った後に、メディアＳＡＭ１３３からメディア鍵データK_{MED}を入力する。

なお、ＳＡＭ１０５$_2$が、事前にメディア鍵データK_{MED}を保持している場合には、当該入力を行わなくても良い。

【０２１２】

ステップＳ５１－２：ＲＯＭ型の記録媒体１３０$_1$のセキュアＲＡＭ領域１３２に記録されているセキュアコンテナ１０４に格納された図３（Ｂ），（Ｃ）に示すキーファイルＫＦおよびその署名データ$SIG_{7,CP}$と、公開鍵証明書データCER_{CP}およびその署名データ$SIG_{1,ESC}$とを、メディア・ドライブＳＡＭ管理部８５５を介して入力して作業用メモリ２００に書き込む。

【０２１３】

ステップＳ５１－３：署名処理部１８９において、署名データ$SIG_{1,ESC}$の正当性を確認した後に、公開鍵証明書データCER_{CP}から公開鍵データ$K_{CP,P}$を取り出し、この公開鍵データ$K_{CP,P}$を用いて、署名データ$SIG_{7,CP}$の正当性、すなわちキーファイルＫＦの送信者の正当性を検証する。

また、署名処理部１８９において、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて、キーファイルＫＦに格納された署名データ$SIG_{K1,ESC}$の正当性、すなわちキーファイルＫＦの作成者の正当性を検証する。

【０２１４】

ステップＳ５１－４：署名処理部１８９において署名データ$SIG_{7,CP}$，$SIG_{K1,ESC}$の正当性が確認されると、作業用メモリ２００から暗号化・復号部１７２にキーファイルＫＦを読み出す。

次に、暗号化・復号部１７２において、対応する期間のライセンス鍵データKD_1～KD_3を用いて、キーファイルＫＦに格納されたコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3を復号した後に、作業用メモリ２００に書き込む。

【０２１５】

ステップＳ５１－５：図５０に示す相互認証部１７０と図４９に示すＡＶ圧縮・伸長用ＳＡＭ１６３との間で相互認証を行った後に、ＳＡＭ105_2のＡＶ圧縮・伸長用ＳＡＭ管理部１８４は、作業用メモリ２００に記憶されているコンテンツ鍵データＫｃおよび権利書データ１０６に格納された半開示パラメータデータ１９９、並びにＲＯＭ型の記録媒体130_1のＲＯＭ領域１３１から読み出したコンテンツファイルＣＦに格納されたコンテンツデータＣを図４９に示すＡＶ圧縮・伸長用ＳＡＭ１６３に出力する。

次に、ＡＶ圧縮・伸長用ＳＡＭ１６３において、コンテンツデータＣがコンテンツ鍵データＫｃを用いて半開示モードで復号された後に伸長され、再生モジュール２７０に出力される。そして、再生モジュール２７０において、ＡＶ圧縮・伸長用ＳＡＭ１６３からのコンテンツデータＣが再生される。

【０２１６】

ステップＳ５１－６：ユーザによる図４９に示す操作部１６５の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す内部割り込みＳ８１０が、ＳＡＭ１０５２のＣＰＵ１１００に出される。

【０２１７】

ステップＳ５１－７：課金処理部１８７は、操作信号Ｓ１６５に応じた利用制御データ１６６を作成し、これを作業用メモリ２００に書き込む。

ステップＳ５１－８：作業用メモリ２００から暗号化・復号部１７３に、コンテンツ鍵データＫｃおよび利用制御データ１６６が出力される。

暗号化・復号部１７３は、作業用メモリ２００から入力したコンテンツ鍵データＫｃおよび利用制御データ１６６を、記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を用いて順次に暗号化して作業用メモリ２００に書き込む。

【０２１８】

ステップＳ５１－９：メディアＳＡＭ管理部１９７において、作業用メモリ２００から読み出した、暗号化されたコンテンツ鍵データＫｃおよび利用制御データ１６６と、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3を

用いて図４４（Ｃ）に示すキーファイル$ＫＦ_1$が生成される。

また、署名処理部１８９において、図４４（Ｃ）に示すキーファイル$ＫＦ_1$のハッシュ値H_{K1}が生成され、当該ハッシュ値H_{K1}がメディア・ドライブＳＡＭ管理部８５５に出力される。

図５０に示す相互認証部１７０と図４９に示すメディアＳＡＭ１３３との間で相互認証を行った後に、メディア・ドライブＳＡＭ管理部８５５は、キーファイル$ＫＦ_1$およびハッシュ値H_{K1}を、図４９に示すメディア・ドラブＳＡＭ２６０を介してＲＯＭ型の記録媒体１３０_1のセキュアＲＡＭ領域１３２に書き込む。

これにより、購入形態が決定されたＲＯＭ型の記録媒体１３０_1が得られる。

このとき、課金処理部１８７が生成した利用制御データ１６６および利用履歴データ１０８は、所定のタイミングで、作業用メモリ２００および外部メモリ２０１からそれぞれ読み出しされたＥＭＤサービスセンタ１０２に送信される。

なお、ＲＯＭ型の記録媒体１３０_1のメディアＳＡＭ１３３にキーファイルＫＦが格納されている場合には、図４９において点線で示されるように、$ＳＡＭ１０５_2$はメディアＳＡＭ１３３からキーファイルＫＦを入力する。また、この場合に、$ＳＡＭ１０５_2$は、作成したキーファイル$ＫＦ_1$をメディアＳＡＭ１３３に書き込む。

【０２１９】

ステップＳ５１－１０：$ＳＡＭ１０５_2$のＣＰＵ１１００は、上述したＲＯＭ型の記録媒体を用いて配給されたコンテツの購入形態を決定する処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述したＲＯＭ型の記録媒体を用いて配給されたコンテツの購入形態を決定する処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０２２０】

＜ＲＯＭ型の記録媒体のコンテンツデータの購入形態を決定した後に、ＲＡＭ型の記録媒体に書き込む場合の処理＞

以下、図５２に示すように、$ＡＶ機器１６０_3$において購入形態が未決定のＲ

ＯＭ型の記録媒体１３０$_1$からセキュアコンテナ１０４を読み出して新たなセキュアコンテナ１０４ｙを生成し、これをＡＶ機器１６０$_2$に転送し、ＡＶ機器１６０$_2$において購入形態を決定してＲＡＭ型の記録媒体１３０$_5$に書き込む際の処理の流れを図５３，図５４，図５５を参照しながら説明する。

なお、ＲＯＭ型の記録媒体１３０$_1$からＲＡＭ型の記録媒体１３０$_5$へのセキュアコンテナ１０４ｙの転送は、図１に示すネットワーク機器１６０$_1$およびＡＶ機器１６０$_1$～１６０$_4$のいずれの間で行ってもよい。

図５５は、当該処理のフローチャートである。

【０２２１】

ステップＳ５５－０：ユーザによる操作部１６５の操作に応じて、購入形態が未決定のＲＯＭ型の記録媒体から読み出したセキュアコンテナをＳＡＭ１０５$_2$に転送することを示す内部割り込みＳ８１０を、図５３に示すＣＰＵ１１００が受ける。

ステップＳ５５－１：ＳＡＭ１０５$_3$は、ＳＡＭ登録リストを検証し、セキュアコンテナの転送先のＳＡＭ１０５$_2$が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ５５－２以降の処理を行う。

また、ＳＡＭ１０５$_3$は、ＳＡＭ１０５$_2$がホームネットワーク内のＳＡＭであるか否かの検証も行う。

ステップＳ５５－２：ＳＡＭ１０５$_3$とＳＡＭ１０５$_2$との間で相互認証が行われ、セッション鍵データK_{SES}が共有される。

【０２２２】

ステップＳ５５－３：ＡＶ機器１６０$_3$のＳＡＭ１０５$_3$とＲＯＭ型の記録媒体１３０$_1$のメディアＳＡＭ１３３との間で相互認証を行い、ＲＯＭ型の記録媒体１３０$_1$のメディア鍵データK_{MED1}をＳＡＭ１０５$_3$に転送する。

なお、メディア鍵データK_{MED1}を用いた暗号化をＲＯＭ型の記録媒体１３０$_1$のメディアＳＡＭ１３３において行う場合には、メディア鍵データK_{MED1}の転送は行わない。

【０２２３】

ステップＳ５５－４：ＡＶ機器１６０$_2$のＳＡＭ１０５$_2$とＲＡＭ型の記録媒体１３０$_5$のメディアＳＡＭ１３３との間で相互認証を行い、ＲＡＭ型の記録媒体１３０$_5$のメディア鍵データK_{MED2}をＳＡＭ１０５$_2$に転送する。

なお、メディア鍵データK_{MED2}を用いた暗号化をＲＡＭ型の記録媒体１３０$_5$のメディアＳＡＭ１３３において行う場合には、メディア鍵データK_{MED2}の転送は行わない。

【０２２４】

ステップＳ５５－５：ＳＡＭ１０５$_3$は、図５３に示すように、メディア・ドライブＳＡＭ管理部８５５を介して、ＲＯＭ型の記録媒体１３０$_1$のＲＯＭ領域１３１からコンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$を読み出し、これをＳＡＭ管理部１９０に出力すると共に、署名処理部１８９において、秘密鍵データ$K_{SAM3,S}$を用いて、これらの署名データ$SIG_{350,SAM3}$を作成する。

【０２２５】

ステップＳ５５－６：ＳＡＭ１０５$_3$は、図５３に示すように、メディア・ドライブＳＡＭ管理部８５５を介して、ＲＯＭ型の記録媒体１３０$_1$のセキュアＲＡＭ領域１３２からキーファイルＫＦおよびその署名データ$SIG_{7,CP}$を読み出し、これをＳＡＭ管理部１９０に出力すると共に、署名処理部１８９において、秘密鍵データ$K_{SAM3,S}$を用いて、これらの署名データ$SIG_{352,SAM3}$が作成される。

【０２２６】

ステップＳ５５－７：ＳＡＭ１０５$_3$において、記憶部１９２からＳＡＭ管理部１９０に公開鍵証明書データCER_{SAM3}およびその署名データ$SIG_{351,ESC}$が読み出される。

【０２２７】

ステップＳ５５－８：ＳＡＭ１０５$_3$の例えばＳＡＭ管理部１９０において、図５４に示すセキュアコンテナ１０４ｙが作成される。

【０２２８】

ステップＳ５５－９：ＳＡＭ１０５$_3$の暗号化・復号部１７１において、ステ

ップＳ５５－２で得たセッション鍵データK_{SES}を用いて、セキュアコンテナ１０４ｙが暗号化される。

【０２２９】

ステップＳ５５－１０：ＳＡＭ１０５$_3$のＳＡＭ管理部１９０からＡＶ機器１６０$_2$に、セキュアコンテナ１０４ｙが出力される。

そして、ＳＡＭ１０５$_3$のＣＰＵ１１００からホストＣＰＵ８１０に、外部割り込みで、上述した処理が適切に行われたか否かが通知される。

なお、ＣＰＵ１１００は、上述した処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

ＳＡＭ１０５$_2$では、ホストＣＰＵ８１０からの内部割り込みＳ８１０によるＣＰＵ１１００の制御によって、図５７に示すように、ＳＡＭ管理部１９０を介してＳＡＭ１０５$_3$から入力した図５４に示すセキュアコンテナ１０４ｙが暗号化・復号部１７１においてセッション鍵データK_{SES}を用いて復号される。

そして、当該復号されたセキュアコンテナ１０４ｙ内のキーファイルＫＦおよびその署名データ$SIG_{7,CP}$、$SIG_{350,SAM3}$と、公開鍵証明書データCER_{SAM3}およびその署名データ$SIG_{351,ESC}$と、公開鍵証明書データCER_{cp}およびその署名データ$SIG_{1,ESC}$とが、作業用メモリ２００に書き込まれる。

【０２３０】

ステップＳ５５－１２：ＳＡＭ１０５$_2$の署名処理部１８９において、セキュアコンテナ１０４ｙ内に格納された署名データ$SIG_{6,CP}$，$SIG_{350,SAM3}$の正当性、すなわちコンテンツファイルＣＦの作成者および送信者の正当性を確認する。

ステップＳ５５－１３：コンテンツファイルＣＦの作成者および送信者が正当であると確認された後に、メディア・ドライブＳＡＭ管理部８５５を介してＲＡＭ型の記録媒体１３０$_5$のＲＡＭ領域１３４にコンテンツファイルＣＦが書き込まれる。

なお、コンテンツファイルＣＦは、ホストＣＰＵ８１０の制御によって、ＳＡＭを介さずに、ＲＡＭ型の記録媒体１３０$_5$のＲＡＭ領域１３４に直接的に記録

してもよい。

【０２３１】

ステップＳ５５－１４：署名処理部１８９において、署名データ$SIG_{351,ECS}$が署名検証され、公開鍵証明書データCER_{SAM3}の正当性が確認された後に、公開鍵証明書データCER_{SAM3}に格納された公開鍵データK_{SAM3}および公開鍵データ$K_{ESC,P}$を用いて、署名データ$SIG_{7,CP}$，$SIG_{352,SAM3}$，$SIG_{K1,ESC}$の正当性、すなわちキーファイルＫＦの作成者および送信者の正当性が確認される。

【０２３２】

ステップＳ５５－１５：キーファイルＫＦの作成者および送信者の正当性が確認されると、作業用メモリ２００からキーファイルＫＦが読み出されて暗号化・復号部１７２に出力され、暗号化・復号部１７２において、ライセンス鍵データKD_1～KD_3を用いて復号された後に、作業用メモリ２００に書き戻される。

【０２３３】

ステップＳ５５－１６：作業用メモリ２００に記憶されている既に復号されたキーファイルＫＦに格納された権利書データ１０６が、利用監視部１８６に出力される。そして、利用監視部１８６において、権利書データ１０６に基づいて、コンテンツの購入形態および利用形態が管理（監視）される。

【０２３４】

ステップＳ５５－１７：ユーザによる図５２に示す操作部１６５の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた内部割り込みＳ８１０が、ホストＣＰＵ８１０からＳＡＭ105_2のＣＰＵ１１００に出される。

ステップＳ５５－１８：課金処理部１８７において、決定された購入・利用形態に応じて利用制御データ１６６および利用履歴データ１０８が生成され、これが作業用メモリ２００および外部メモリ２０１にそれぞれ書き込まれる。

利用制御データ１６６および利用履歴データ１０８は、所定のタイミングで、ＥＭＤサービスセンタ１０２に送信される。

【０２３５】

ステップＳ５５－１９：コンテンツ鍵データＫｃおよび利用制御データ１６６

が、作業用メモリ２００から暗号化・復号部１７３に読み出され、暗号化・復号部１７３において記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED2}および購入者鍵データK_{PIN}を用いて順に暗号化され、メディアＳＡＭ管理部１９７に出力される。

また、作業用メモリ２００からメディアＳＡＭ管理部１９７に、キーファイルＫＦが出力される。

【０２３６】

ステップＳ５５－２０：メディアＳＡＭ管理部１９７において、図４４（Ｃ）に示すキーファイルKF_1が作成され、キーファイルKF_1がメディアＳＡＭ管理部１９７を介してＲＡＭ型の記録媒体130_5のメディアＳＡＭ１３３に書き込まれる。

また、メディアＳＡＭ管理部１９７を介して、キーファイルＫＦがＲＡＭ型の記録媒体130_5のメディアＳＡＭ１３３に書き込まれる。

【０２３７】

ステップＳ５５－２１：$SAM105_2$のＣＰＵ１１００は、上述した処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述した処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０２３８】

以下、$SAM105_1$～105_4の実現方法について説明する。

$SAM105_1$～105_4の機能をハードウェアとして実現する場合は、メモリを内蔵したＡＳＩＣ型のＣＰＵを用いて、そのメモリには、図２２に示す各機能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密度の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【０２３９】

例えば、図２２に示す暗号化・復号部１７１などのモジュールは、例えば、処理速度の問題でハードウエアとしてＡＳＩＣ型のＣＰＵ内のＩＰコアとして実装される。クロック速度やＣＰＵコード体系などの性能によっては、暗号化・復号部１７１をソフトウェアとして実装してもよい。

また、図２２に示す記憶部１９２や、図２２に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリー（フラッシューＲＯＭ）が用いられ、作業用メモリとしてはＳＲＡＭなどの高速書き込み可能なメモリが用いられる。なお、その他にも、ＳＡＭ105_1～105_4に内蔵されるメモリとして、強誘電体メモリー（ＦｅＲＡＭ）を用いてもよい。

また、ＳＡＭ105_1～105_4には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【０２４０】

上述したように、ＳＡＭ105_1～105_4は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。ＳＡＭ105_1～105_4を搭載した機器のホストＣＰＵのバス経由で、当該ＳＡＭのＩＣ内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、ＳＡＭのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストＣＰＵが割り付けているアドレス空間内に存在しないように、当該ＳＡＭでは、ＣＰＵ側のメモリー空間を管理するＭＭＵ(Memory Magagement Unit)を用いて、搭載機器側のホストＣＰＵからは見えないアドレス空間を設定する。

また、ＳＡＭ105_1～105_4は、Ｘ線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウエアＩＣＥ、ソフトウエアＩＣＥ）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがＩＣ製造後には使用できないような構造をしている。

ＳＡＭ１０５$_1$～１０５$_4$自身は、ハードウエア的な構造においては、メモリを内蔵した通常のＡＳＩＣ型のＣＰＵであり、機能は当該ＣＰＵを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なＡＳＩＣ型のＣＰＵと異なる。

【０２４１】

ＳＡＭ１０５$_1$～１０５$_4$の機能を全てソフトウエアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウエア処理を行う場合と、通常のセットに搭載されているホストＣＰＵ上のソフトウエア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがＩＰコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ＩＣＥ（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（ＭｉｎｉＯＳ）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【０２４２】

次に、図２２に示すＡＶ圧縮・伸長用ＳＡＭ１６３について説明する。

図２２に示すように、ＡＶ圧縮・伸長用ＳＡＭ１６３は、相互認証部２２０、復号部２２１、復号部２２２、伸長部２２３、電子透かし情報処理部２２４および半開示処理部２２５を有する。

相互認証部２２０は、ＡＶ圧縮・伸長用ＳＡＭ１６３がＳＡＭ１０５$_1$からデータを入力する際に、図３０に示す相互認証部１７０との間で相互認証を行ってセッション鍵データK_{SES}を生成する。

【０２４３】

復号部２２１は、ＳＡＭ１０５$_1$から入力したコンテンツ鍵データＫｃ、半開示パラメータデータ１９９、ユーザ電子透かし情報用データ１９６およびコンテ

ンツデータＣを、セッション鍵データK_{SES}を用いて復号する。そして、復号部２２１は、復号したコンテンツ鍵データＫｃおよびコンテンツデータＣを復号部２２２に出力し、復号したユーザ電子透かし情報用データ１９６を電子透かし情報処理部２２４に出力し、半開示パラメータデータ１９９を半開示処理部２２５に出力する。

【０２４４】

復号部２２２は、半開示処理部２２５からの制御に基づいて、コンテンツ鍵データＫｃを用いて、コンテンツデータＣを半開示状態で復号し、復号したコンテンツデータＣを伸長部２２３に出力する。

また、復号部２２２は、通常動作時にコンテンツデータＣの全体をコンテンツ鍵データＫｃで復号する。

【０２４５】

伸長部２２３は、復号されたコンテンツデータＣを伸長して、電子透かし情報処理部２２４に出力する。

伸長部２２３は、例えば、図３（Ａ）に示すコンテンツファイルＣＦに格納されたＡ／Ｖ伸長用ソフトウェアを用いて伸長処理を行い、例えば、ＡＴＲＡＣ３方式で伸長処理を行う。

【０２４６】

電子透かし情報処理部２２４は、復号されたユーザ電子透かし情報用データ１９６に応じたユーザ電子透かし情報を、復号されたコンテンツデータＣに埋め込み、新たなコンテンツデータＣを生成する。電子透かし情報処理部２２４は、当該新たなコンテンツデータＣを再生モジュール１６９に出力する。

このように、ユーザ電子透かし情報は、コンテンツデータＣを再生するときに、ＡＶ圧縮・伸長用ＳＡＭ１６３において埋め込まれる。

なお、本発明では、コンテンツデータＣにユーザ電子透かし情報用データ１９６を埋め込まないようにしてもよい。

【０２４７】

半開示処理部２２５は、半開示パラメータデータ１９９に基づいて、例えば、コンテンツデータＣのうち復号を行わないブロックと、復号を行うブロックとを

復号部２２２に指示する。

また、半開示処理部２２５は、その他に、半開示パラメータデータ１９９に基づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【０２４８】

再生モジュール１６９は、復号および伸長されたコンテンツデータＣに応じた再生を行う。

【０２４９】

以下、ＳＡＭ１０５$_1$～１０５$_4$の出荷時におけるＥＭＤサービスセンタ１０２への登録処理について説明する。

なお、ＳＡＭ１０５$_1$～１０５$_4$の登録処理は同じであるため、以下、ＳＡＭ１０５$_1$の登録処理について述べる。

ＳＡＭ１０５$_1$の出荷時には、ＥＭＤサービスセンタ１０２の鍵サーバ１４１によって、ＳＡＭ管理部１４９を介して、図３０などに示す記憶部１９２に以下に示す鍵データが初期登録される。

また、ＳＡＭ１０５$_1$には、例えば、出荷時に、記憶部１９２などに、ＳＡＭ１０５$_1$がＥＭＤサービスセンタ１０２に初回にアクセスする際に用いられるプログラムなどが記憶される。

すなわち、記憶部１９２には、例えば、図３４において左側に「＊」が付されているＳＡＭ１０５$_1$の識別子ＳＡＭ＿ＩＤ、記録用鍵データK_{STR}、ルート認証局２の公開鍵データK_{R-CA}、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,S}$、公開鍵証明書データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$、ＡＶ圧縮・伸長用ＳＡＭ１６３およびメディアＳＡＭとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶される。

なお、公開鍵証明書データCER_{SAM1}は、ＳＡＭ１０５$_1$を出荷後に登録する際にＥＭＤサービスセンタ１０２からＳＡＭ１０５$_1$に送信してもよい。

【０２５０】

また、記憶部１９２には、ＳＡＭ１０５$_1$の出荷時に、図３に示すコンテンツ

ファイルＣＦおよびキーファイルＫＦを読み込み形式を示すファイルリーダが、ＥＭＤサービスセンタ１０２によって書き込まれる。

ＳＡＭ１０５$_1$では、コンテンツファイルＣＦおよびキーファイルＫＦに格納されたデータを利用する際に、記憶部１９２に記憶されたファイルリーダが用いられる。

【０２５１】

ここで、ルート認証局２の公開鍵データK_{R-CA}は、インターネットの電子商取引などでは一般的に使用されているＲＳＡを使用し、データ長は例えば１０２４ビットである。公開鍵データK_{R-CA}は、図１に示すルート認証局２によって発行される。

また、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$は、短いデータ長でＲＳＡと同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば１６０ビットである。但し、暗号化の強度を考慮すると、公開鍵データ$K_{ESC,P}$は１９２ビット以上であることが望ましい。また、ＥＭＤサービスセンタ１０２は、ルート認証局９２に公開鍵データ$K_{ESC,P}$を登録する。

また、ルート認証局９２は、公開鍵データ$K_{ESC,P}$の公開鍵証明書データCER_{ESC}を作成する。公開鍵データ$K_{ESC,P}$を格納した公開鍵証明書データCER_{ESC}は、好ましく、ＳＡＭ１０５$_1$の出荷時に記憶部１９２に記憶される。この場合に、公開鍵証明書データCER_{ESC}は、ルート認証局９２の秘密鍵データ$K_{ROOT,S}$で署名されている。

【０２５２】

ＥＭＤサービスセンタ１０２は、乱数を発生してＳＡＭ１０５$_1$の秘密鍵データ$K_{SAM1,S}$を生成し、これとペアとなる公開鍵データ$K_{SAM1,P}$を生成する。

また、ＥＭＤサービスセンタ１０２は、ルート認証局９２の認証をもらって、公開鍵データ$K_{SAM1,P}$の公開鍵証明書データCER_{SAM1}を発行し、これに自らの秘密鍵データ$K_{ESC,S}$を用いて署名データを添付する。すなわち、ＥＭＤサービスセンタ１０２は、セカンドＣＡ（認証局）として機能を果たす。

【０２５３】

また、ＳＡＭ１０５$_1$には、ＥＭＤサービスセンタ１０２により、ＥＭＤサー

ビスセンタ１０２の管理下にある一意（ユニーク）な識別子ＳＡＭ＿ＩＤが割り当てられ、これがＳＡＭ１０５$_1$ の記憶部１９２に格納されると共に、ＥＭＤサービスセンタ１０２によって管理される。

【０２５４】

また、ＳＡＭ１０５$_1$ は、出荷後、例えば、ユーザによってＥＭＤサービスセンタ１０２と接続され、登録手続を行うと共に、ＥＭＤサービスセンタ１０２から記憶部１９２にライセンス鍵データＫＤ$_1$ ～ＫＤ$_3$ が転送される。

すなわち、ＳＡＭ１０５$_1$ を利用するユーザは、コンテンツをダウンロードする前にＥＭＤサービスセンタ１０２に登録手続が必要である。この登録手続は、例えば、ＳＡＭ１０５$_1$ を搭載している機器（当該例では、ネットワーク機器１６０$_1$ ）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報（ユーザの氏名、住所、連絡先、性別、決済口座、ログイン名、パスワードなど）を記載して例えば郵便などのオフラインで行なわれる。

ＳＡＭ１０５$_1$ は、上述した登録手続を経た後でないと使用できない。

【０２５５】

ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$ のユーザによる登録手続に応じて、ユーザに固有の識別子ＵＳＥＲ＿ＩＤを発行し、例えば、ＳＡＭ＿ＩＤとＵＳＥＲ＿ＩＤとの対応関係を管理し、課金時に利用する。

また、ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$ のユーザに対して情報参照用識別子ＩＤと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子ＩＤとパスワードとを用いて、ＥＭＤサービスセンタ１０２に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。

また、ＥＭＤサービスセンタ１０２は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

【０２５６】

次に、図３４に示すように、ＳＡＭ１０５$_1$ 内の記憶部１９２にＳＡＭ登録リストを格納する手順について説明する。

図１に示すＳＡＭ１０５$_1$ は、例えば、バス１９１としてＩＥＥＥ１３９４シ

リアルバスを用いた場合に、バス１９１に接続された機器の電源を立ち上げたり、新しい機器をバス１９１に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するＳＡＭ１０５$_2$～ＳＡＭ１０５$_4$のＳＡＭ登録リストを得る。

なお、ＩＥＥＥ１３９４シリアルバスであるバス１９１に応じて生成されたトポロジーマップは、例えば、図５８に示すように、バス１９１にＳＡＭ１０５$_1$～１０５$_4$に加えてＡＶ機器１６０$_5$，１６０$_6$のＳＣＭＳ処理回路１０５$_5$，１０５$_6$が接続されている場合に、ＳＡＭ１０５$_1$～１０５$_4$およびＳＣＭＳ処理回路１０５$_5$，１０５$_6$を対象として生成される。

従って、ＳＡＭ１０５$_1$は、当該トポロジーマップから、ＳＡＭ１０５$_1$～１０５$_4$についての情報を抽出して図５９に示すＳＡＭ登録リストを生成する。

【０２５７】

そして、ＳＡＭ１０５$_1$は、図５９に示すＳＡＭ登録リストを、ＥＭＤサービスセンタ１０２に登録して署名を得る。

これらの処理は、バス１９１のセッションを利用してＳＡＭ１０５$_1$が自動的に行い、ＥＭＤサービスセンタ１０２にＳＡＭ登録リストの登録命令を発行する。

ＥＭＤサービスセンタ１０２は、ＳＡＭ１０５$_1$から図５９に示すＳＡＭ登録リストを受けると、有効期限を確認する。そして、ＥＭＤサービスセンタ１０２は、登録時にＳＡＭ１０５$_1$より指定された決済機能の有無を参照して対応する部分の設定を行う。また、ＥＭＤサービスセンタ１０２は、予め保持している図６０に示すリボケーションリストＣＲＬをチェックしてＳＡＭ登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にＥＭＤサービスセンタ１０２によって使用が禁止されている（無効な）ＳＡＭのリストである。各ＳＡＭは他のＳＡＭと通信を行う際に、リボケーションリストによって通信相手のＳＡＭが無効にされている場合には、当該通信相手のＳＡＭとの通信を停止する。

また、ＥＭＤサービスセンタ１０２は、決済時にはＳＡＭ１０５$_1$に対応するＳＡＭ登録リストを取り出し、その中に記述されたＳＡＭがリボケーションリス

トに含まれているかを確認する。また、ＥＭＤサービスセンタ１０２は、ＳＡＭ登録リストに署名を添付する。

これにより、図６１に示すＳＡＭ登録リストが作成される。

なお、ＳＡＭリボケーションリストは、同一系の（同一のバス１９１に接続されている）ＳＡＭのみを対象として生成され、各ＳＡＭに対応するリボケーションンフラグによって、当該ＳＡＭの有効および無効を示している。

【０２５８】

なお、リボケーションリストＣＲＬの更新は、例えば、ＥＭＤサービスセンタ１０２からＳＡＭに放送される更新データに応じて、ＳＡＭ内部で自動的に行なうことが好ましい。

【０２５９】

以下、ＳＡＭが持つセキュリティ機能について説明する。

ＳＡＭは、セキュリティに関する機能として、共通鍵暗号方式のＤＥＳ（Triple DES/AES）、公開鍵暗号方式の楕円曲線暗号（署名生成／検証ＥＣ－ＤＳＡ，共有鍵生成ＥＣ－Ｄ．Ｈ．，公開鍵暗号ＥＣ－Elgamal），圧縮関数のハッシュ関数ＳＨＡ－１，乱数生成器（真性乱数）の暗号ライブラリーのＩＰ部品を有している。

相互認証、署名生成、署名検証、共有鍵（セッション鍵）作成（配送）には公開鍵暗号方式（楕円曲線暗号）が用いられ、コンテンツの暗号、復号には共通鍵暗号（ＤＥＳ）が用いられ、署名生成、検証の中のメッセージ認証に圧縮関数（ハッシュ関数）が用いられる。

【０２６０】

図６２は、ＳＡＭが持つセキュリティ機能を説明するための図である。

ＳＡＭが管理するセキュリティー機能は、コンテンツに関連する暗号、復号処理をつかさどるアプリケーション層でのセキュリティー機能（１）と、通信相手と相互認証をしてセキュアな通信路を確保する物理層のセキュリティー機能（２）との２種類がある。

ＥＭＤシステム１００では、配信されるコンテンツデータＣはすべて暗号化され、決済と同時に鍵の購入手続きをすることを前提としている。権利書データ１

０６は、コンテンツデータＣと一緒にイン・バンド方式で送られることを前提としているので、ネットワークの媒体と関係のない層でそのデータが管理され、衛星、地上波、ケーブル、無線、記録媒体（メディア）などの流通経路によらず、共通な権利処理システムを提供できる。具体的には、権利書データ１０６をネットワークの物理層のプロトコルのヘッダに挿入したりすると、使用するネットワークによって、挿入するデータが同じでも、ヘッダのどこに挿入するかを各々のネットワークで決めないといけない。

【０２６１】

本実施形態では、コンテンツデータＣおよびキーファイルＫＦの暗号化は、アプリケーション層での保護を意味している。相互認証は、物理層やトランスポート層で行ってもよいし、アプリケーション層で行ってもよい。物理層に暗号機能を組み込むことは、使用するハードウエアに暗号機能を組み込むことを意味している。送信、受信の両者間のセキュアの通信路を確保することが相互認証の本来の目的なので物理層で実現できることが望ましいが、実際はトランスポート層で実現し、伝送路によらないレベルでの相互認証が多い。

【０２６２】

ＳＡＭが実現するセキュリティ機能には、通信先の相手の正当性を確認するための相互認証と、アプリケーション層での課金処理をともなうコンテンツデータの暗号化および復号とがある。

機器間で通信を行う際のＳＡＭ相互間での相互認証は、通常、アプリケーション層レベルに実装されるが、トランスポート層や物理層などの他のレイヤに実装されてもよい。

物理層に実装する相互認証は、５Ｃ１３９４ＣＰ（Content Protection）を利用する。１３９４ＣＰは１３９４ＬＩＮＫＩＣ（ハードウエア）のIsochronous Channel に共通鍵暗号であるＭ６が実装されてあり、Asynchronous Channelによる相互認証（楕円曲線暗号、ハッシュ関数を利用した共通鍵暗号）の結果、生成されるセッション鍵をIsochronous Channel のＭ６に転送し、Ｍ６による共通鍵暗号を実現する。

【０２６３】

ＳＡＭ相互間の相互認証を物理層のハードウエア上に実装する場合には、公開鍵暗号（楕円曲線暗号）を利用した相互認証で生成されたセッション鍵をホストＣＰＵを介して１３９４ＬＩＮＫＩＣのＭ６に転送し、１３９４ＣＰで生成されたセッション鍵と併用してコンテンツデータの暗号化を行う。

また、ＳＡＭ相互間の相互認証をアプリケーション層で行う場合には、ＳＡＭ内部の共通鍵暗号ライブラリ(DES/Triple DES/AES)を使って暗号化を行う。

【０２６４】

本実施形態では、例えば、ＳＡＭ相互間の相互認証をアプリケーション層に実装し、１３９４ＣＰによる相互認証を１３９４ＬＩＮＫＩＣという物理層（ハードウエア）に実装する。

この場合に、課金処理をともなうコンテンツデータの暗号化および復号はアプリケーション層で行われるが、アプリケーション層は一般ユーザから簡単にアクセスでき、時間無制限に解析される可能性があるため、当該課金処理をともなう処理に関しては、本実施形態では、外部から処理内容をいっさいモニタ（監視）できない耐タンパ性をもったハードウエア内部で行っている。これがＳＡＭを耐タンパ性の構造を持ったハードウエアで実現する最大の理由である。

なお、当該課金処理をホストＣＰＵ内で行う場合は、ＣＰＵに耐タンパ性のソフトウェアを実装する。

【０２６５】

以下、図１に示すユーザホームネットワーク１０３内の例えばネットワーク機器160_1内での各種のＳＡＭに搭載形態の一例を図６３を参照しながら説明する。

図６３に示すように、ネットワーク機器160_1内には、ホストＣＰＵ810_1、$SAM105_1$、ダウンロードメモリ１６７、メディア・ドラブＳＡＭ２６０、ドライブＣＰＵ１００３、ＤＲＡＭなどのショックプルーフ(Shock Proof：耐振動用）メモリ１００４を有する。

ダウンロードメモリ１６７と、ショックプルーフメモリ１００４の一部の記憶領域は、$SAM105_1$および$ホストCPU810_1$の双方からアクセス可能な

共有メモリとして用いられる。

ショックプルーフメモリ１００４は、データバス１００２を介して入力したコンテンツデータを蓄積した後にＡＶ圧縮・伸長用ＳＡＭ１６３に出力することで、記録媒体１３０からのコンテンツデータの読み出し動作が振動などに要因で途切れた場合でも、ＡＶ圧縮・伸長用ＳＡＭ１６３に連続してコンテンツデータＣを出力することを可能にする。これによって、コンテンツデータの再生出力が途切れることが効果的に回避される。

【０２６６】

ダウンロードメモリ１６７は、メモリコントローラ、バスアービターおよびブリッジの機能を持つモジュール１００５を介して、ホストＣＰＵバス１０００に接続されている。

図６４は、モジュール１００５の内部およびその周辺の構成を詳細に示した図である。

図６４に示すように、モジュール１００５は、コントローラ１５００およびバスアービタ／バスブリッジ１５０１を有する。

コントローラ１５００は、ダウンロードメモリ１６７としてＤＲＡＭを用いた場合に、ＤＲＡＭＩ／Ｆとして機能し、ダウンロードメモリ１６７との間にｒ／ｗ線、アドレスバス、ＣＡＳ¯線およびＲＡＳ¯線を有している。

バスアービタ／バスブリッジ１５０１は、ホストＣＰＵバス１０００のアービトレーション等を行い、ダウンロードメモリ１６７との間にデータバスを有し、コントローラ１５００との間にｒ／ｗ線、アドレスバスおよびＲｅａｄｙ線を有し、ＳＡＭ１０５１との間にＣＳ(Chip Select)線、ｒ／ｗ線、アドレスバス、データバスおよびＲｅａｄｙ線を有し、ホストＣＰＵバス１０００に接続されている。

ホストＣＰＵバス１０００には、バスアービタ／バスブリッジ１５０１、ホストＣＰＵ８１０$_1$およびＳＡＭ１０５$_1$が接続されている。

ホストＣＰＵバス１０００は、ＣＳ線、ｒ／ｗ線、アドレスバス、データバスおよびＲｅａｄｙ線を有する。

【０２６７】

ダウンロードメモリ１６７およびショックプルーフメモリ１００４には、前述したコンテンツファイルＣＦおよびキーファイルＫＦなどが記憶される。

ショックプルーフメモリ１００４の記憶領域のうち共有メモリとしては用いられる記憶領域以外の記憶領域は、データバス１００２を介してメディア・ドラブＳＡＭ２６０から入力したコンテンツデータをＡＶ圧縮・伸長用ＳＡＭ１６３に出力するまで一時的に記憶するために用いられる。

【０２６８】

ＡＶ圧縮・伸長用ＳＡＭ１６３は、ホストＣＰＵバス１０００を介してダウンロードメモリ１６７との間でデータ転送を行い、データバス１００２を介してメディア・ドラブＳＡＭ２６０との間でデータ転送を行う。

【０２６９】

ホストＣＰＵバス１０００には、ダウンロードメモリ１６７の他に、ＳＡＭ１０５$_1$、ＡＶ圧縮・伸長用ＳＡＭ１６３およびＤＭＡ(Direct Memory Access)１０１０が接続されている。

ＤＭＡ１０１０は、ホストＣＰＵバス１０００を介したダウンロードメモリ１６７へのアクセスを、ホストＣＰＵ８１０$_1$からの命令に応じて、統括的に制御する。

また、ホストＣＰＵバス１０００は、１３９４シリアル・インターフェースのＬＩＮＫ層を用いてユーザホームネットワーク１０３内の他のＳＡＭ１０５$_2$～１０５$_4$と通信を行なう際に用いられる。

【０２７０】

ドライブＣＰＵバス１００１には、ドライブＣＰＵ１００３、メディア・ドラブＳＡＭ２６０、ＲＦアンプ１００６、メディアＳＡＭインターフェイス１００７およびＤＭＡ１０１１が接続されている。

ドライブＣＰＵ１００３は、例えば、ホストＣＰＵ８１０$_1$からの命令を受けて、ディスク型の記録媒体１３０にアクセスを行う際の処理を統括的に制御する。この場合に、ホストＣＰＵ８１０$_1$がマスタとなり、ドライブＣＰＵ１００３がスレーブとなる。ドライブＣＰＵ１００３は、ホストＣＰＵ８１０$_1$から見て

Ｉ／Ｏとして扱われる。

ドライブＣＰＵ１００３は、例えばＲＡＭ型などの記録媒体１３０にアクセスを行う際のデータのエンコードおよびデコードを行う。

ドライブＣＰＵ１００３は、ＲＡＭ型の記録媒体１３０がドライブにセットされると、ＲＡＭ型の記録媒体１３０がＳＡＭ１０５$_1$ による権利処理の対象となる（ＥＭＤシステム１００の対象となる）記録媒体であるか否かを判断し、当該記録媒体であると判断した場合に、そのことをホストＣＰＵ８１０$_1$ に通知すると共に、メディア・ドラブＳＡＭ２６０にメディアＳＡＭ１３３との間の相互認証などを行うことを指示する。

【０２７１】

メディアＳＡＭインターフェイス１００７は、ドライブＣＰＵバス１００１を介した記録媒体１３０のメディアＳＡＭ１３３に対してのアクセスを行う際のインターフェイスとして機能する。

ＤＭＡ１０１１は、例えば、ドライブＣＰＵ１００３からの命令に応じて、ドライブＣＰＵバス１００１およびデータバス１００２を介したショックプルーフメモリ１００４へのメモリアクセスを統括的に制御する。ＤＭＡ１０１１は、例えば、データバス１００２を介した、メディア・ドラブＳＡＭ２６０とショックプルーフメモリ１００４との間のデータ転送を制御する。

【０２７２】

図６３に示す構成では、例えば、ＳＡＭ１０５$_1$ と記録媒体１３０のメディアＳＡＭ１３３との間で相互認証などの通信を場合には、ホストＣＰＵ８１０$_1$ の制御に基づいて、ホストＣＰＵバス１０００、ホストＣＰＵ８１０$_1$ 、ドライブＣＰＵ１００３内のレジスタ、ドライブＣＰＵバス１００１およびメディアＳＡＭインターフェイス１００７を介して、ＳＡＭ１０５$_1$ とメディアＳＡＭ１３３との間でデータが転送される。

また、記録媒体１３０にアクセスを行う場合には、メディア・ドラブＳＡＭ２６０とメディアＳＡＭ１３３との間で相互認証が行われる。

また、前述したように、ダウンロードメモリ１６７およびショックプルーフメモリ１００４にアクセスを行うために、ＡＶ圧縮・伸長用ＳＡＭ１６３において

データを圧縮または伸長する場合には、ＳＡＭ１０５$_1$とＡＶ圧縮・伸長用ＳＡＭ１６３との間で相互認証が行われる。

【０２７３】

本実施形態では、図６３において、ＳＡＭ１０５$_1$およびＡＶ圧縮・伸長用ＳＡＭ１６３は、ホストＣＰＵ８１０$_1$からは、Ｉ／Ｏインターフェイスに接続されたデバイスとして扱われる。ＳＡＭ１０５$_1$およびＡＶ圧縮・伸長用ＳＡＭ１６３とホストＣＰＵ８１０$_1$との間の通信およびデータ転送は、メモリＩ／Ｏ＆アドレスデコーダ１０２０の制御に基づいて行われる。このとき、ホストＣＰＵ８１０$_1$がマスタ(Master)になり、ＳＡＭ１０５$_1$およびＡＶ圧縮・伸長用ＳＡＭ１６３がスレーブ(Slave)になる。ＳＡＭ１０５$_1$およびＡＶ圧縮・伸長用ＳＡＭ１６３は、ホストＣＰＵ８１０$_1$からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をホストＣＰＵ８１０$_1$に通知する。

また、メディアＳＡＭ１３３およびメディア・ドラブＳＡＭ２６０は、ドライブＣＰＵ１００３からはＩ／Ｏインターフェイスに接続されたデバイスとして扱われる。メディアＳＡＭ１３３およびメディア・ドラブＳＡＭ２６０とドライブＣＰＵ１００３との間の通信およびデータ転送は、メモリＩ／Ｏ＆アドレスデコーダ１０２１の制御に基づいて行われる。このとき、ドライブＣＰＵ１００３がマスタになり、メディアＳＡＭ１３３およびメディア・ドラブＳＡＭ２６０がスレーブになる。メディアＳＡＭ１３３およびメディア・ドラブＳＡＭ２６０は、ドライブＣＰＵ１００３からの命令に基づいて要求された処理を行い、必要に応じて、当該処理の結果をドライブＣＰＵ１００３に通知する。

【０２７４】

また、ダウンロードメモリ１６７およびショックプルーフメモリ１００４に対してのコンテンツファイルＣＦおよびキーファイルＫＦに関するアクセス制御は、ＳＡＭ１０５$_1$が統括的に行ってもよいし、あるいはコンテンツファイルＣＦのアクセス制御をホストＣＰＵ８１０$_1$が行い、キーファイルＫＦのアクセス制御をＳＡＭ１０５$_1$が行ってもよい。

【０２７５】

ドライブＣＰＵ１００３によって記録媒体１３０から読み出されたコンテンツ

データＣは、ＲＦアンプ１００６およびメディア・ドラブＳＡＭ２６０を経て、ショックプルーフメモリ１００４に格納され、その後、ＡＶ圧縮・伸長用ＳＡＭ１６３において伸長される。伸長されたコンテンツデータはＤ／Ａ変換器におい、２てデジタルからアナログに変換され、当該変換によって得られたアナログ信号に応じた音響がスピーカから出力される。

このとき、ショックプルーフメモリ１００４は、記録媒体１３０の離散的に位置する記録領域から非連続的に読み出された複数のトラックのコンテンツデータＣを一時的に格納した後に、ＡＶ圧縮・伸長用ＳＡＭ１６３に連続して出力してもよい。

【０２７６】

以下、図６３に示すユーザホームネットワーク１０３内の各種のＳＡＭのマスタ・スレーブ関係を説明する。

例えば、購入形態を決定したコンテンツデータを記録媒体１３０に記録する場合には、図６５に示すように、ホストＣＰＵ８１$０_1$ が、そのＩ／Ｏデバイスである$ＳＡＭ１０５_1$ に、当該コンテンツデータの購入形態決定を行う旨を内部割り込みによって指示すると共に、記録媒体１３０のメディアＳＡＭ１３３と相互認証を行って、記録媒体１３０にコンテンツデータを記録する。

このとき、ホストＣＰＵ８$１０_1$ がマスタとなり、$ＳＡＭ１０５_1$ および記録媒体１３０がスレーブとなる。記録媒体１３０も、ホストＣＰＵ８$１０_1$ からはＩ／Ｏデバイスとして扱われる。

$ＳＡＭ１０５_1$ は、ホストＣＰＵ８$１０_1$ から上記内部割り込みを受けると、記録媒体１３０のメディアＳＡＭ１３３と通信を行って、コンテンツデータの購入形態を決定すると共に、コンテンツ鍵データＫｃなどの所定の鍵データをメディアＳＡＭ１３３に書き込む。そして、$ＳＡＭ１０５_1$ は、当該処理が終了すると、ホストＣＰＵ８$１０_1$ に対しての外部割り込み、あるいはホストＣＰＵ８$１０_1$ からのポーリングによって、当該処理の結果をホストＣＰＵ８$１０_1$ に通知する。

【０２７７】

また、例えば、記録媒体に記録された既に購入形態が決定されたコンテンツデ

ータの再生を行う場合には、図６６に示すように、ホストＣＰＵ８１０$_1$からＳＡＭ１０５$_1$に対して、当該再生を行う旨の指示が内部割り込みによって出される。

ＳＡＭ１０５$_1$は、当該内部割り込みを受けると、記録媒体１３０のメディアＳＡＭ１３３からキーファイルＫＦなどの鍵データブロックを読み出し、当該鍵データブロックに格納された利用制御データ１６６などに基づいて、コンテンツデータの再生処理を行う。

ＳＡＭ１０５$_1$は、ＡＶ圧縮・伸長用ＳＡＭ１６３に、記録媒体１３０から読み出したコンテンツデータの伸長処理を行う旨の指示を内部割り込みによって出す。

ＡＶ圧縮・伸長用ＳＡＭ１６３は、当該内部割り込みをＳＡＭ１０５$_1$から受けると、記録媒体１３０から読み出したコンテンツデータのデスクランブル処理、電子透かし情報の埋め込み処理および検出処理、並びに伸長処理を行った後に、当該コンテンツデータをＤ／Ａ変換回路などを介して出力して再生を行う。

そして、ＡＶ圧縮・伸長用ＳＡＭ１６３は、当該再生処理が終了すると、その旨をＳＡＭ１０５$_1$に通知する。

ＳＡＭ１０５$_1$は、ＡＶ圧縮・伸長用ＳＡＭ１６３から、当該再生処理が終了した旨の通知を受けると、その旨を外部割り込み等でホストＣＰＵ８１０$_1$に通知する。

この場合に、ホストＣＰＵ８１０$_1$とＳＡＭ１０５$_1$との関係では、ホストＣＰＵ８１０$_1$がマスタとなり、ＳＡＭ１０５$_1$がスレーブとなる。

また、ＳＡＭ１０５$_1$とＡＶ圧縮・伸長用ＳＡＭ１６３との関係では、ＳＡＭ１０５$_1$がマスタとなり、ＡＶ圧縮・伸長用ＳＡＭ１６３がスレーブとなる。

また、上述した実施形態では、ＡＶ圧縮・伸長用ＳＡＭ１６３をＳＡＭ１０５$_1$のスレーブとなるようにしたが、ＡＶ圧縮・伸長用ＳＡＭ１６３をホストＣＰＵ８１０$_1$のスレーブとなるようにしてもよい。

【０２７８】

また、例えば、コンテンツデータの権利処理を行うことなく、記録媒体１３０に記録されたコンテンツデータの再生処理を行う場合には、図６７に示すように

、ホストＣＰＵ８１０$_1$からＡＶ圧縮・伸長用ＳＡＭ１６３に、内部割り込みによって、再生処理を行う旨の指示が出される。また、ホストＣＰＵ８１０$_1$からメディア・ドラブＳＡＭ２６０に、内部割り込みによって、記録媒体１３０からコンテンツデータを読み出す旨の指示が出される。

メディア・ドラブＳＡＭ２６０は、上記内部割り込みを受けると、記録媒体１３０から読み出したコンテンツデータをデコード部でデコードした後に、ショックプルーフメモリ１００４に格納する。そして、メディア・ドラブＳＡＭ２６０は、当該処理を終了すると、その旨を外部割り込みによってホストＣＰＵ８１０$_1$に通知する。

ショックプルーフメモリ１００４に格納されたコンテンツデータは、ＡＶ圧縮・伸長用ＳＡＭ１６３によって読み出され、ＡＶ圧縮・伸長用ＳＡＭ１６３において、デスクランブル処理、電子透かし情報の埋め込み処理および検出処理、並びに伸長処理を行った後に、Ｄ／Ａ変換回路などを介して再生出力される。

ＡＶ圧縮・伸長用ＳＡＭ１６３は、当該再生処理が終了すると、その旨を外部割り込みによってホストＣＰＵ８１０$_1$に通知する。

この場合に、ホストＣＰＵ８１０$_1$がマスタとなり、ＡＶ圧縮・伸長用ＳＡＭ１６３およびメディア・ドラブＳＡＭ２６０がスレーブとなる。

【０２７９】

以下、ユーザホームネットワーク１０３内の各種のＳＡＭが上述した機能を実現するために備える回路モジュールについて説明する。

ユーザホームネットワーク１０３内のＳＡＭとしては、前述したように、購入形態の決定などの権利処理（利益分配）に係わる処理を行うＳＡＭ１０５（１０５$_1$～１０５$_4$）と、記録媒体に設けられるメディアＳＡＭ１３３と、ＡＶ圧縮・伸長用ＳＡＭ１６３と、メディア・ドラブＳＡＭ２６０とがある。以下、これらのＳＡＭに設けられる回路モジュールをそれぞれ説明する。

【０２８０】

＜権利処理用のＳＡＭの第１形態＞

図６８は、権利処理用のＳＡＭ１０５ａの回路モジュールを説明するための図である。

図６８に示すように、ＳＡＭ１０５ａは、ＣＰＵ１１００、ＤＭＡ１１０１、ＭＭＵ１１０２、Ｉ／Ｏモジュール１１０３、マスクＲＯＭ１１０４、不揮発性メモリ１１０５、作業用ＲＡＭ１１０６、公開鍵暗号モジュール１１０７、共通鍵暗号モジュール１１０８、ハッシュ関数モジュール１１０９、（真性）乱数発生器１１１０、リアルタイムクロックモジュール１１１１、外部バスＩ／Ｆ１１１２を有する耐タンパ性のハードウェア(Tamper Registant H/W)（本発明の回路モジュール）である。

ここで、ＣＰＵ１１００が本発明の演算処理回路に対応し、マスクＲＯＭ１１０４、不揮発性メモリ１１０５および作業用ＲＡＭ１１０６が本発明の記憶回路に対応し、共通鍵暗号モジュール１１０８が本発明の暗号処理回路に対応し、外部バスＩ／Ｆ１１１２が本発明の外部バスインターフェイスに対応している。

また、後述する図６４の内部バス１１２０，１１２１が本発明の第１のバスに対応し、外部バス１１２３が本発明の第２のバスに対応している。

また、内部バス１１２０が本発明の第３のバスに対応し、内部バス１１２１が本発明の第４のバスに対応している。

また、外部バスＩ／Ｆ１１１２が本発明の第１のインターフェイス回路に対応し、バスＩ／Ｆ回路１１１６が本発明の第２のインターフェイス回路に対応している。

また、内部バス１１２２が本発明の第５のバスに対応し、Ｉ／Ｏモジュールが本発明の第３のインターフェイス回路に対応し、バスＩ／Ｆ回路１１１７が本発明の第４のインターフェイス回路に対応している。

【０２８１】

図３０に示すＳＡＭ105_1の機能モジュールと、図６８に示す回路モジュールとの関係を簡単に説明する。

ＣＰＵ１１００は、例えば、マスクＲＯＭ１１０４および不揮発性メモリ１１０５に記憶されたプログラムを実行して、図３０に示すＣＰＵ１１００、課金処理部１８７および利用監視部１８６の機能を実現する。

ＤＭＡ１１０１は、ＣＰＵ１１００からの命令に応じて、図２２に示すダウンロードメモリ１６７および図３０に示す記憶部１９２に対してのアクセスを統括

的に制御する。

ＭＭＵ１１０２は、図２２に示すダウンロードメモリ１６７および図３０に示す記憶部１９２のアドレス空間を管理する。

Ｉ／Ｏモジュール１１０３は、例えば、図３０に示すメディアＳＡＭ管理部１９７の一部の機能を実現する。

マスクＲＯＭ１１０４には、ＳＡＭ１０５ａの初期化プログラムやインテグリティチェック(Integrity Check) プログラムなどの改変しないプログラムおよびデータが製造時に記憶され、図３０に示す記憶部１９２の一部の機能を実現する。

不揮発性メモリ１１０５は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶し、図３０に示す記憶部１９２の一部の機能を実現する。

作業用ＲＡＭ１１０６は、図３０に示す作業用メモリ２００に対応している。

【０２８２】

公開鍵暗号モジュール１１０７は、図３０に示す署名処理部１８９の機能の一部を実現し、例えば、公開鍵暗号方式を用いた、メディアＳＡＭ１３３等と間の相互認証、ＳＡＭ１０５の署名データの作成、署名データ（ＥＭＤサービスセンタ１０２、コンテンツプロバイダ１０１、第２実施形態の場合にはサービスプロバイダ３１０の署名データ）の検証、データ量の少ないデータ（キーファイルＫＦなど）の転送を行う際の当該データの暗号化および復号、並びに、鍵共有を行う際に用いられる。公開鍵暗号モジュール１１０７は、回路モジュールとして実現してもよいし(H/W IP Solution) 、不揮発性メモリ１１０５に記憶した公開鍵暗号プログラムをＣＰＵ１１００において実行して実現してもよい(S/W IPSolution)。

【０２８３】

共通鍵暗号モジュール１１０８は、図３０に示す署名処理部１８９、暗号化・復号部１７１，１７２，１７３の機能の一部を実現し、相互認証、相互認証によって得た共通鍵であるセッション鍵データK_{SES}を用いたデータの暗号化および復号を行う際に用いられる。共通鍵暗号方式は、公開鍵暗号方式に比べて高速処理が可能であり、例えば、コンテンツデータ（コンテンツファイルＣＦ）などの

データ量が大きいデータを暗号化および復号する際に用いられる。共通鍵暗号モジュール１１０８は、回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ１１０５に記憶した共通鍵暗号プログラムをＣＰＵ１１００において実行して実現してもよい(S/W IP Solution)。

なお、相互認証は、公開鍵暗号モジュール１１０７による暗号・復号および共通鍵暗号モジュール１１０８による暗号・復号の何れか一方あるいは双方を採用する。

また、共通鍵暗号モジュール１１０８は、コンテンツ鍵データＫｃをライセンス鍵データＫＤを用いて復号する。

【０２８４】

ハッシュ関数モジュール１１０９は、図３０に示す署名処理部１８９の機能の一部を実現し、署名データを作成する対象となるデータのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール１１０９は、コンテンツプロバイダ１０１およびＥＭＤサービスセンタ１０２などの署名データや、図４４に示すセキュアコンテナ１０４ｘのキーファイルKF_1のハッシュ値H_{K1}を検証する際に用いられる。ハッシュ関数モジュール１１０９は、回路モジュールとして実現してもよいし(H/W IPSolution)、不揮発性メモリ１１０５に記憶したハッシュ回路モジュールをＣＰＵ１１００において実行して実現してもよい(S/W IP Solution)。

【０２８５】

乱数発生器１１１０は、例えば、図３０に示す相互認証部１７０の機能の一部を実現する。

リアルタイムクロックモジュール１１１１は、リアルタイムの時刻を発生する。当該時刻は、例えば、有効期限付きのライセンス鍵データＫＤを選択する場合や、利用制御データ１６６によって示される有効期限の要件を満たされているか否かを判断する際に用いられる。

外部バスＩ／Ｆ１１１２は、図３０に示すコンテンツプロバイダ管理部１８０、ダウンロードメモリ管理部１８２およびＥＭＤサービスセンタ管理部１８５の一部を機能を実現する。

【０２８６】

図６９は、ＳＡＭ１０５ａ内のハードウェア構成を説明するための図である。

図６９において、図６８に示したものと同じ回路モジュールには、図６８と同じ符号を付している。

図６９に示すように、ＳＡＭ１０５ａ内では、ＳＡＭ・ＣＰＵバス１１２０を介してＣＰＵ１１００、マスクＲＯＭ１１０４および不揮発性メモリ１１０５が接続されている。

内部バス１１２１には、ＤＭＡ１１０１が接続されている。

内部バス１１２２には、I^2C・インターフェイス１１３０、メディアＳＡＭ・インターフェイス１１３１、ＭＳ(Memory Stick)・インターフェイス１１３２およびＩＣカード・インターフェイス１１３３が接続されている。

メディアＳＡＭ・インターフェイス１１３１は記録媒体１３０のメディアＳＡＭ１３３との間でデータ転送を行う。ＭＳ・インターフェイス１１３２はメモリスティック１１４０との間でデータ転送を行う。ＩＣカード・インターフェイス１１３３はＩＣカード１１４１との間でデータ転送を行う。

【０２８７】

外部バス１１２３には、公開鍵暗号モジュール１１０７、共通鍵暗号モジュール１１０８、ハッシュ関数モジュール１１０９、乱数発生器１１１０、リアルタイムクロック生成モジュール１１１１、外部バスＩ／Ｆ１１１２および外部メモリＩ／Ｆ１１４０が接続されている。

外部バスＩ／Ｆ１１１２は、図６３に示す外部メモリ２０１が接続される。

外部メモリＩ／Ｆ１１４０は、図６３に示すホストＣＰＵバス１０００に接続される。

【０２８８】

ＳＡＭ・ＣＰＵバス１１２０と内部バス１１２１とは、バス・インターフェイス１１６を介して接続されている。

内部バス１１２２と内部バス１１２１とは、バス・インターフェイス１１１７を介して接続されている。

内部バス１１２１と外部バス１１２３とは、バス・インターフェイス１１１５

を介して接続されている。

【０２８９】

バス・インターフェイス１１１５内には、ＳＲＡＭ１１５５およびＳＡＭステータスレジスタ１１５６が設けられている。

ＳＲＡＭ１１５５は、後述するように、

ＳＡＭステータスレジスタ１１５６には、前述したように、第１のＳＡＭステータスレジスタおよび第２のＳＡＭステータスレジスタがある。第１のＳＡＭステータスレジスタには、ホストＣＰＵ８１０$_1$によって読み出される、ＳＡＭ１０５$_1$のステータス（状態）を示すフラグが設定される。第２のＳＡＭステータスレジスタには、ホストＣＰＵ８１０$_1$からタスク実行の依頼が出されているか否かのステータスをＳＡＭ１０５$_1$の内部のＣＰＵから読みにいくフラグが設定される。

【０２９０】

ＤＭＡ１１０１は、ＣＰＵ１１００からの命令に応じて、内部バス１１２１を介した、マスクＲＯＭ１１０４、不揮発性メモリ１１０５および作業用ＲＡＭ１１０６に対してのアクセスを統括的に制御する。

ＭＭＵ１１１３は、マスクＲＯＭ１１０４、不揮発性メモリ１１０５、作業用ＲＡＭ１１０６、図６３に示すダウンロードメモリ１６７のメモリ空間を管理する。

アドレスデコーダ１１１４は、内部バス１１２１と外部バス１１２３との間でデータ転送を行う際に、アドレス変換を行う。

また、書き込みロック制御回路１１３５は、ＣＰＵ１１００からのロック鍵データに基づいて、フラッシュＲＯＭに対してのデータの書き込みおよび消去をブロック単位で管理する。

【０２９１】

次に、権利処理用のＳＡＭ１０５ａのアドレス空間を説明する。

図７０は、権利処理用のＳＡＭ１０５ａのアドレス空間を説明するための図である。

図７０に示すように、権利処理用のＳＡＭ１０５ａのアドレス空間には、開始

アドレスから順に、例えば、ブートプログラム、システムコンフィギュレーション、フラッシュＲＯＭ、所定のプログラム、フラッシュＲＯＭのデバイスドライバ、不揮発性メモリのデバイスドライバ、図６９に示す作業用ＲＡＭ１１０６、所定のプログラム、作業用ＲＡＭ１１０６、所定のプログラム、図６９に示すＳＲＡＭ１１５５、外部メモリ２０１、Ｋｅｙ＿ＴＯＣ／Ｆｉｌｅ＿Ｓｙｓｔｅｍ、ＳＡＭ登録リスト、利用履歴データ１０８、図６９に示す共通鍵暗号モジュール１１０８のレジスタ、図６９に示す公開鍵暗号モジュール１１０７のレジスタ、図６９に示すハッシュ関数モジュール１１０９のレジスタ、図６９に示す乱数発生器１１１０のレジスタ、図６９に示すリアルタイムクロックモジュール１１１１のレジスタ、現在時刻レジスタ、有効期限レジスタ、コントロールレジスタ、ＩＣカードのインターフェイス、メディアＳＡＭのインターフェイス、メモリスティックのインターフェイス、I^2Cバスのインターフェイスに割り当てられている。

【０２９２】

システムコンフィギュレーションに割り当てられたアドレス空間内には、図６９に示すＤＭＡ１１０１およびＳＡＭステータスレジスタ１１５６が割り当てられている。

また、フラッシュＲＯＭに割り当てられたアドレス空間内には、メインルーチン（カーネル）、割り込みプログラム、当該割り込みプログラムによって呼び出されるサブルーチン、コマンド解析部（コマンドと割り込みプログラムの開始アドレスの対応表）、割り込みベクタテーブルが割り当てられている。

図７０に示すＳＡＭ１０５ａのアドレス空間のうち、ＳＡＭステータスレジスタ１１５６およびＳＲＡＭ１１５５は、ホストＣＰＵ８１０との共有メモリ空間として用いられる。

【０２９３】

次に、図６３に示すホストＣＰＵ８１０_1のアドレス空間を説明する。

図７１は、図６３に示すホストＣＰＵ８１０_1のアドレス空間を説明するための図である。

図７１に示すように、ホストＣＰＵ８１０_1のアドレス空間は、開始アドレス

から順に、例えば、ブートプログラム、システムコンフィギュレーション、コードが記憶されるＲＯＭ、データが記憶されるＲＡＭ、作業用ＲＡＭ、図６３に示すＳＡＭ１０５$_1$との共有メモリ、図６３に示すＡＶ圧縮・伸長用ＳＡＭ１６３との共有メモリ、図６３に示すメディア・ドラブＳＡＭ２６０との共有メモリおよび外部デバイスが割り当てられている。

図６３に示すＳＡＭ１０５$_1$との共有メモリには、図６９に示すＳＲＡＭ１１５５およびＳＡＭステータスレジスタ１１５６が割り当てられている。

【０２９４】

＜権利処理用のＳＡＭの第２形態＞

図７２は、権利処理用のＳＡＭ１０５ｂの回路モジュールを説明するための図である。

図７２では、ＳＡＭ１０５ａの構成要素と同じものには、図６９と同じ符号を付している。

図７２に示すように、ＳＡＭ１０５ｂは、セキュアメモリ１０５ｂａ、ホストＣＰＵ８１０、耐タンパ性ソフトウェア１１３０、Ｉ／Ｏモジュール１１０３を用いて実現される。

ＳＡＭ１０５ｂでは、ホストＣＰＵ８１０において、耐タンパ性ソフトウェア１１３０を実行することで、図６８に示すＣＰＵ１１００と同じ機能を実現する。耐タンパ性ソフトウェア１１３０は、前述したように、耐タンパ性を持ったモジュール内部で閉じたソフトウェアであり、解読および書き換え困難なソフトウェアである。

セキュアメモリ１０５ｂａには、マスクＲＯＭ１１０４、不揮発性メモリ１１０５、作業用ＲＡＭ１１０６、公開鍵暗号モジュール１１０７、共通鍵暗号モジュール１１０８、ハッシュ関数モジュール１１０９、（真性）乱数発生器１１１０、リアルタイムクロックモジュール１１１１および外部バスＩ／Ｆ１１１２を有する耐タンパ性のハードウェアである。

なお、公開鍵暗号モジュール１１０７、共通鍵暗号モジュール１１０８およびハッシュ関数モジュール１１０９は、回路モジュールとして実現してもよいし(H/W IP Solution)、それぞれ不揮発性メモリ１１０５に記憶した公開鍵暗号プロ

グラム、共通鍵暗号プログラムおよびハッシュ関数プログラムをホストＣＰＵ８１０において実行して実現してもよい(S/W IP Solution)。

【０２９５】

以下、前述したメディアＳＡＭ１３３の構成の一例を説明する。

図７３は、メディアＳＡＭ１３３の回路モジュールを説明するための図である。

図７３に示すように、メディアＳＡＭ１３３は、ＣＰＵ１２００、ＤＭＡ１２０１、Ｉ／Ｏモジュール１２０３、マスクＲＯＭ１２０４、不揮発性メモリ１２０５、作業用ＲＡＭ１２０６、公開鍵暗号モジュール１２０７、共通鍵暗号モジュール１２０８、ハッシュ関数モジュール１２０９、（真性）乱数発生器１２１０を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【０２９６】

ＣＰＵ１２００は、耐タンパ性のハードウェア内の各回路の制御を行う。

【０２９７】

作業用ＲＡＭ１１０６は、図３０に示す作業用メモリ２００に対応している。

公開鍵暗号モジュール１２０７は、例えば、公開鍵暗号方式を用いた、例えば（１）：図６３に示すＳＡＭ１０５$_1$ およびドライブＣＰＵ１００３等と間の相互認証、（２）メディアＳＡＭ１３３の署名データの作成、署名データ（ＥＭＤサービスセンタ１０２、コンテンツプロバイダ１０１、第２実施形態の場合にはサービスプロバイダ３１０の署名データ）の検証、（３）：転送されるデータ量の少ないメッセージの暗号化および復号、並びに、（４）：相互認証によって得たセッション鍵データK_{SES} の鍵共有を行う際に用いられる。公開鍵暗号モジュール１１０７は、回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ１２０５に記憶した公開鍵暗号プログラムをＣＰＵ１２００において実行して実現してもよい(S/W IPSolution)。

【０２９８】

共通鍵暗号モジュール１２０８は、相互認証、相互認証によって得た共通鍵であるセッション鍵データK_{SES} を用いたキーファイルＫＦ，KF_1 などのデータの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール１２０８は、

回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ１２０５に記憶した共通鍵暗号プログラムをＣＰＵ１２００において実行して実現してもよい(S/W IP Solution)。

なお、相互認証は、公開鍵暗号モジュール１２０７による暗号・復号および共通鍵暗号モジュール１２０８による暗号・復号の何れか一方あるいは双方を採用する。

【０２９９】

ハッシュ関数モジュール１２０９は、データのハッシュ値を生成する際に用いられる。具体的には、ハッシュ関数モジュール１１０９は、図４４に示すセキュアコンテナ１０４ｘのキーファイルKF_1のハッシュ値H_{K1}を検証する際に用いられる。ハッシュ関数モジュール１２０９は、回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ１２０５に記憶したハッシュ回路モジュールをＣＰＵ１２００において実行して実現してもよい(S/W IP Solution)。

【０３００】

乱数発生器１２１０は、例えば、相互認証を行う際に用いられる。

Ｉ／Ｏモジュール１２０３は、図６３に示すメディアＳＡＭＩ／Ｆ１００７との間の通信を行う際に用いられる。

【０３０１】

マスクＲＯＭ１２０４には、メディアＳＡＭ１３３の初期化プログラムやインテグリティチェック(Integrity Check)プログラムなどの改変しないプログラムおよびデータが製造時に記憶される。

不揮発性メモリ１２０５は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。

【０３０２】

図７４は、メディアＳＡＭ１３３がＲＯＭ型の記録媒体に搭載される場合に、メディアＳＡＭ１３３の出荷時にマスクＲＯＭ１２０４および不揮発性メモリ１２０５に格納されているデータを示す図である。

図７４に示すように、ＲＯＭ型の記録媒体の出荷時には、メディアＳＡＭ１３

３には、メディアＳＡＭの識別子（ＩＤ）、記録用鍵データK_{STR}（メディア鍵データK_{MED}）、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ルート認証局９２の公開鍵データ$K_{R-CA,P}$、メディアＳＡＭ１３３の公開鍵証明書データCER_{MSAM}，メディアＳＡＭ１３３の公開鍵データ$K_{MSAM,P}$、メディアＳＡＭ１３３の秘密鍵データ$K_{MSAM,S}$、リボケーションリスト、権利処理用データ、利益分配したいエンティティの識別子（ＩＤ）、メディアのタイプ（メディアの種別情報、ＲＯＭおよびＲＡＭの何れかを特定する情報）、キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ、所定の検証値（ＭＡＣ値）などが記憶される。

ここで、キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ、並びに所定の検証値（ＭＡＣ値）は、ＥＭＤサービスセンタ１０２が管理するライセンス鍵データＫＤを用いて暗号化されている。

【０３０３】

図７５は、メディアＳＡＭ１３３がＲＯＭ型の記録媒体に搭載される場合に、メディアＳＡＭ１３３の出荷後のユーザ登録およびコンテンツデータの購入形態決定を行ったときにマスクＲＯＭ１２０４および不揮発性メモリ１２０５に格納されているデータを示す図である。

図７５に示すように、メディアＳＡＭ１３３には、ユーザ登録によって、新たに、ユーザＩＤ、パスワード、個人嗜好情報、個人決済情報（クレジットカード番号など）および電子マネー情報、キーファイルKF_1などのデータが書き込まれる。

【０３０４】

図７６は、メディアＳＡＭ１３３がＲＡＭ型の記録媒体に搭載される場合に、メディアＳＡＭ１３３の出荷時にマスクＲＯＭ１２０４および不揮発性メモリ１２０５に格納されているデータを示す図である。

図７６に示すように、ＲＡＭ型の記録媒体の出荷時には、メディアＳＡＭ１３３には、メディアＳＡＭの識別子（ＩＤ）、記録用鍵データK_{STR}（メディア鍵

データK_{MED}）、ＥＭＤサービスセンタ１０２の公開鍵データ$K_{ESC,P}$、ルート認証局９２の公開鍵データ$K_{R-CA,P}$、メディアＳＡＭ１３３の公開鍵証明書データＣＥＲ$_{MSAM}$、メディアＳＡＭ１３３の公開鍵データ$K_{MSAM,P}$、メディアＳＡＭ１３３の秘密鍵データ$K_{MSAM,S}$、リボケーションリスト、権利処理用データ、利益分配したいエンティティの識別子（ＩＤ）、メディアのタイプ（メディアの種別情報、ＲＯＭおよびＲＡＭの何れかを特定する情報）が記憶されており、キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ，KF_1、所定の検証値（ＭＡＣ値）などは記憶されていない。

【０３０５】

図７７は、メディアＳＡＭ１３３がＲＡＭ型の記録媒体に搭載される場合に、メディアＳＡＭ１３３の出荷後のユーザ登録およびコンテンツデータの購入形態決定処理を行ったときにマスクＲＯＭ１２０４および不揮発性メモリ１２０５に格納されているデータを示す図である。

図７３に示すように、メディアＳＡＭ１３３には、ユーザ登録によって、新たに、ユーザＩＤ、パスワード、個人嗜好情報、個人決済情報（クレジットカード番号など）および電子マネー情報などのデータに加えて、キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ，KF_1、並びに所定の検証値（ＭＡＣ値）が書き込まれる。

キーファイルＫＦの物理アドレス情報（レジスタ空間のアドレス）、各コンテンツデータＣ（コンテンツファイルＣＦ）のキーファイルＫＦ，KF_1、並びに所定の検証値（ＭＡＣ値）は、記録用鍵データK_{STR}によって暗号化されている。

【０３０６】

＜ＡＶ圧縮・伸長用ＳＡＭ１６３＞

ＡＶ圧縮・伸長用ＳＡＭ１６３は、例えば、図２２を用いて説明した機能を実現する。

図７８は、ＡＶ圧縮・伸長用ＳＡＭ１６３の回路モジュールを説明するための

図である。

図７８に示すように、ＡＶ圧縮・伸長用ＳＡＭ１６３は、ＣＰＵ／ＤＳＰ１３００、ＤＭＡ１３０１、マスクＲＯＭ１３０４、不揮発性メモリ１３０５、作業用ＲＡＭ１３０６、共通鍵暗号モジュール１３０８、（真性）乱数発生器１３１０、圧縮・伸長モジュール１３２０、電子透かし情報付加・検出モジュール１３２１および情報半開示制御モジュール１３２２を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【０３０７】

ＣＰＵ／ＤＳＰ１３００は、例えば、図６３に示すＳＡＭ１０５$_1$からの命令に応じて、マスクＲＯＭ１３０４および不揮発性メモリ１３０５に記憶されたプログラムを実行し、ＡＶ圧縮・伸長用ＳＡＭ１６３内の各回路モジュールを統括的に制御する。

ＤＭＡ１３０１は、ＣＰＵ／ＤＳＰ１３００からの命令に応じて、マスクＲＯＭ１３０４、不揮発性メモリ１３０５、作業用ＲＡＭ１３０６に対してのアクセスを統括的に制御する。

マスクＲＯＭ１３０４には、ＡＶ圧縮・伸長用ＳＡＭ１６３の初期化プログラムやインテグリティチェック(Integrity Check) プログラムなどの改変しないプログラムや、ＡＶ圧縮・伸長用ＳＡＭ１６３の識別子であるＡＶＳＡＭ__ＩＤなどの改変しないデータが製造時に記憶される。

不揮発性メモリ１３０５は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。

作業用ＲＡＭ１３０６は、ＳＡＭ１０５$_1$から入力したキーファイルＫＦなどを記憶する。

【０３０８】

共通鍵暗号モジュール１３０８は、ＳＡＭ１０５$_1$との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データK_{SES}を用いたコンテンツデータおよびコンテンツ鍵データＫｃなどの暗号化および復号を行う際に用いられる。共通鍵暗号モジュール１３０８は、回路モジュールとして実現してもよいし(H/W IP Solution)、不揮発性メモリ１３０５に記憶した共通鍵暗号プログラムを

ＣＰＵ／ＤＳＰ１３００において実行して実現してもよい(S/W IP Solution)。

また、共通鍵暗号モジュール１３０８は、$SAM105_1$から得たコンテンツ鍵データＫｃを用いて、コンテンツデータＣの復号を行う。

乱数発生器１１１０は、例えば、$SAM105_1$との間の相互認証処理を行う際に用いられる。

【０３０９】

圧縮・伸長モジュール１３２０は、例えば、図２２に示す伸長部２２３の機能を実現し、図６３に示すダウンロードメモリ１６７およびショックプルーフメモリ１００４から入力したコンテンツデータの伸長処理と、Ａ／Ｄ変換器から入力したコンテンツデータの圧縮処理とを行う。

【０３１０】

電子透かし情報添付・検出モジュール１３２１は、図２２に示す電子透かし情報処理部２２４の機能を実現し、例えば、圧縮・伸長モジュール１３２０の処理対象となるコンテンツデータに対して所定の電子透かし情報を埋め込むと共に、当該コンテンツデータに埋め込まれた電子透かし情報を検出し、圧縮・伸長モジュール１３２０による処理の適否を判断する。

【０３１１】

情報半開示制御モジュール１３２２は、図２２に示す半開示処理部２２５の機能を実現し、必要に応じて、コンテンツデータを半開示状態で再生する。

【０３１２】

＜メディア・ドラブＳＡＭ２６０＞

図７９は、メディア・ドラブＳＡＭ２６０の回路モジュールを説明するための図である。

図７９に示すように、メディア・ドラブＳＡＭ２６０は、ＣＰＵ１４００、ＤＭＡ１４０１、マスクＲＯＭ１４０４、不揮発性メモリ１４０５、作業用ＲＡＭ１４０６、共通鍵暗号モジュール１４０８、ハッシュ関数モジュール１４０９、（真性）乱数発生器１４１０、エンコーダ・デコーダモジュール１４２０、記録用鍵データ生成モジュール１４３０およびメディア・ユニークＩＤ生成モジュール１４４０を有する耐タンパ性のハードウェア(Tamper Registant H/W)である。

【０３１３】

ＣＰＵ１４００は、例えば、図６３に示すドライブＣＰＵ１００３からの命令に応じて、マスクＲＯＭ１４０４および不揮発性メモリ１４０５に記憶されたプログラムを実行し、メディア・ドラブＳＡＭ２６０内の各回路モジュールを統括的に制御する。

ＤＭＡ１４０１は、ＣＰＵ１４００からの命令に応じて、マスクＲＯＭ１４０４、不揮発性メモリ１４０５、作業用ＲＡＭ１４０６に対してのアクセスを統括的に制御する。

マスクＲＯＭ１４０４には、メディア・ドラブＳＡＭ２６０の初期化プログラムやインテグリティチェック(Integrity Check) プログラムなどの改変しないプログラムや、メディア・ドラブＳＡＭ２６０の識別子であるＭＤＳＡＭ＿ＩＤなどの改変しないデータが製造時に記憶される。

不揮発性メモリ１４０５は、改変する可能性のある例えば暗号化プログラムや鍵データなどを記憶する。

作業用ＲＡＭ１４０６は、種々の処理を行う際の作業用メモリとして用いられる。

【０３１４】

共通鍵暗号モジュール１４０８は、メディアＳＡＭ１３３およびＡＶ圧縮・伸長用ＳＡＭ１６３との間の相互認証、相互認証によって得た共通鍵であるセッション鍵データK_{SES}を用いたコンテンツファイルＣＦおよびキーファイルＫＦなどの暗号化および復号、並びに記録用鍵データK_{STR}およびメディア鍵データK_{MED}を用いたコンテンツ鍵データＫｃの暗号化などを行う際に用いられる。また、共通鍵暗号モジュール１４０８は、共通鍵データと署名の対象となるデータのハッシュ値を用いて、署名データの検証および作成を行う。

共通鍵暗号モジュール１４０８は、回路モジュールとして実現してもよいし(H/W IPSolution)、不揮発性メモリ１４０５に記憶した共通鍵暗号プログラムをＣＰＵ１４００において実行して実現してもよい(S/W IP Solution) 。

なお、記録用鍵データK_{STR}を用いたコンテンツ鍵データＫｃの暗号化は、メディア・ドラブＳＡＭ２６０の共通鍵暗号モジュール１４０８およびメディアＳ

ＡＭ１３３の何れで行ってもよい。

ハッシュ関数モジュール１４０９は、署名データの検証、並びに署名データを作成する対象となるデータのハッシュ値を生成する際に用いられる。

乱数発生器１４１０は、例えば、メディアＳＡＭ１３３との間の相互認証処理を行う際に用いられる。

【０３１５】

エンコーダ・デコーダモジュール１４２０は、記録媒体１３０のＲＯＭ領域あるいはＲＡＭ領域に対して、コンテンツデータのアクセスを行う際に、当該コンテンツデータのエンコード処理、デコード処理、ＥＣＣ(Error Correction Code)処理、変調処理、復調処理、セクタライズ処理およびデセクタライズ処理などを行う。

【０３１６】

記録用鍵データ生成モジュール１４３０は、メディア・ユニークＩＤ生成モジュール１４４０が生成したメディア・ユニークＩＤを用いて、各メディアにユニークな記録用鍵データK_{STR}を生成する。

【０３１７】

メディア・ユニークＩＤ生成モジュール１４４０は、メディア・ドラブＳＡＭ２６０で生成したドライブＩＤと、メディアＳＡＭ１３３のメディアＳＡＭ＿ＩＤとから、各記録媒体（メディア）にユニークなメディア・ユニークＩＤを生成する。

【０３１８】

以下、図１に示すＥＭＤシステム１００の全体動作について説明する。

図８０は、コンテンツプロバイダ１０１の全体動作のフローチャートである。

ステップＳ１：ＥＭＤサービスセンタ１０２は、コンテンツプロバイダ１０１が所定の登録処理を経た後に、コンテンツプロバイダ１０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}をコンテンツプロバイダ１０１に送信する。

また、ＥＭＤサービスセンタ１０２は、$SAM105_1$～105_4が所定の登録処理を経た後に、$SAM105_1$～105_4の公開鍵データ$K_{SAM1,P}$～$K_{SAM4,P}$の公開鍵証明書CER_{CP1}～CER_{CP4}を$SAM105_1$～105_4に送信す

る。

また、ＥＭＤサービスセンタ１０２は、相互認証を行った後に、各々有効期限が１カ月の３カ月分のライセンス鍵データKD_1～KD_3をユーザホームネットワーク１０３のＳＡＭ105_1～105_4に送信する。

このように、ＥＭＤシステム１００では、ライセンス鍵データKD_1～KD_3を予めＳＡＭ105_1～105_4に配給しているため、ＳＡＭ105_1～105_4とＥＭＤサービスセンタ１０２との間がオフラインの状態でも、ＳＡＭ105_1～105_4においてコンテンツプロバイダ１０１から配給されたセキュアコンテナ１０４を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ１０８に記述され、利用履歴データ１０８は、ＳＡＭ105_1～105_4とＥＭＤサービスセンタ１０２とが接続されたときに、ＥＭＤサービスセンタ１０２に自動的に送信されるため、ＥＭＤサービスセンタ１０２における決済処理を確実に行うことができる。なお、ＥＭＤサービスセンタ１０２が、所定の期間内に、利用履歴データ１０８を回収できないＳＡＭについては、リボケーションリストで無効の対象とする。

なお、利用制御状態データ１６６は、原則として、リアルタイムで、ＳＡＭ105_1～105_4からＥＭＤサービスセンタ１０２に送信される。

【０３１９】

ステップＳ２：コンテンツプロバイダ１０１は、ＥＭＤサービスセンタ１０２との間で相互認証を行った後に、権利書データ１０６およびコンテンツ鍵データＫｃをＥＭＤサービスセンタ１０２に登録して権威化する。

また、ＥＭＤサービスセンタ１０２は、６カ月分のキーファイルＫＦを作成し、これをコンテンツプロバイダ１０１に送信する。

【０３２０】

ステップＳ３：コンテンツプロバイダ１０１は、図３（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$と、キーファイルＫＦおよびその署名データ$SIG_{7,CP}$とを作成し、これらと図３（Ｃ）に示す公開鍵証明書データCER_{cp}およびその署名データ$SIG_{1,ESC}$とを格納したセキュアコンテナ１０４を、オンラインおよび／またはオフラインで、ユーザホームネット

ワーク１０３のＳＡＭ１０５$_1$ ～１０５$_4$ に配給する。

オンラインの場合には、コンテンツプロバイダ用配送プロトコルを用いられ、当該プロトコルに依存しない形式で（すなわち、複数階層からなる通信プロトコルの所定の層を用いて伝送されるデータとして）、セキュアコンテナ１０４がコンテンツプロバイダ１０１からユーザホームネットワーク１０３に配送される。また、オフラインの場合には、ＲＯＭ型あるいはＲＡＭ型の記録媒体に記録された状態で、セキュアコンテナ１０４が、コンテンツプロバイダ１０１からユーザホームネットワーク１０３に配送される。

【０３２１】

ステップＳ４：ユーザホームネットワーク１０３のＳＡＭ１０５$_1$ ～ＳＡＭ１０５$_4$ は、コンテンツプロバイダ１０１から配給を受けたセキュアコンテナ１０４内の署名データ$SIG_{6,CP}$，$SIG_{7,CP}$，$SIG_{K1,ESC}$を検証して、コンテンツファイルＣＦおよびキーファイルＫＦの作成者および送信者の正当性を確認した後に、対応する期間のライセンス鍵データＫＤ$_1$ ～ＫＤ$_6$ を用いてキーファイルＫＦを復号する。

【０３２２】

ステップＳ５：ＳＡＭ１０５$_1$ ～ＳＡＭ１０５$_4$ において、ユーザによる図２２に示す操作部１６５の操作に応じたホストＣＰＵ８１０からの内部割り込みＳ８１０に基づいて、購入・利用形態を決定する。

このとき、図３７に示す利用監視部１８６において、セキュアコンテナ１０４に格納された権利書データ１０６に基づいて、ユーザによるコンテンツファイルＣＦの購入・利用形態が管理される。

【０３２３】

ステップＳ６：ＳＡＭ１０５$_1$ ～ＳＡＭ１０５$_4$ の図３７に示す課金処理部１８７において、ユーザによる購入・利用形態の決定の操作を記述した利用履歴データ１０８および利用制御状態データ１６６が生成し、これらをＥＭＤサービスセンタ１０２に送信する。

【０３２４】

ステップＳ７：ＥＭＤサービスセンタ１０２は、利用履歴データ１０８に基づ

いて決済処理を行い、決済請求権データ１５２および決済レポートデータ１０７を作成する。ＥＭＤサービスセンタ１０２は、決済請求権データ１５２およびその署名データ$ＳＩＧ_{99}$を、図１に示すペイメントゲートウェイ９０を介して、決済機関９１に送信する。また、ＥＭＤサービスセンタ１０２は、決済レポートデータ１０７をコンテンツプロバイダ１０１に送信する。

【０３２５】

ステップＳ８：　決済機関９１において、署名データ$ＳＩＧ_{99}$の検証を行った後に、決済請求権データ１５２に基づいて、ユーザが支払った金額が、コンテンツプロバイダ１０１の所有者に分配される。

【０３２６】

以上説明したように、ＥＭＤシステム１００では、図３に示すフォーマットのセキュアコンテナ１０４をコンテンツプロバイダ１０１からユーザホームネットワーク１０３に配給し、セキュアコンテナ１０４内のキーファイルＫＦについての処理を$ＳＡＭ１０５_1$～１０５_4内で行う。

また、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６は、配信鍵データ$ＫＤ_1$～$ＫＤ_3$を用いて暗号化されており、配信鍵データ$ＫＤ_1$～$ＫＤ_3$を保持している$ＳＡＭ１０５_1$～１０５_4内でのみ復号される。そして、$ＳＡＭ１０５_1$～１０５_4では、耐タンパ性を有するモジュールであり、権利書データ１０６に記述されたコンテンツデータＣの取り扱い内容に基づいて、コンテンツデータＣの購入形態および利用形態が決定される。

従って、ＥＭＤシステム１００によれば、ユーザホームネットワーク１０３におけるコンテンツデータＣの購入および利用を、コンテンツプロバイダ１０１の関係者が作成した権利書データ１０６の内容に基づいて確実に行わせることができる。

【０３２７】

また、ＥＭＤシステム１００では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３へのコンテンツデータＣの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ１０４を用いて行うことで、$ＳＡＭ１０５_1$～１０５_4におけるコンテンツデータＣの権利処理を双方の場合におい

て共通化できる。

【０３２８】

また、ＥＭＤシステム１００では、ユーザホームネットワーク１０３内のネットワーク機器160_1およびＡＶ機器160_2～160_4においてコンテンツデータＣを購入、利用、記録および転送する際に、常に権利書データ１０６に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【０３２９】

図８１は、第１実施形態で採用されるセキュアコンテナの配送プロトコルの一例を説明するための図である。

図８１に示すように、マルチプロセッサシステム１００では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３にセキュアコンテナ１０４を配送するプロトコルとして例えばＴＣＰ／ＩＰおよびXML／ＳＭＩＬが用いられる。

また、ユーザホームネットワーク１０３のＳＡＭ相互間でセキュアコンテナを転送するプロトコル、並びにユーザホームネットワーク１０３と１０３ａとの間でセキュアコンテナを転送するプロトコルとして例えば１３９４シリアルバス・インタフェース上に構築されたXML／ＳＭＩＬが用いられる。また、この場合に、ＲＯＭ型やＲＡＭ型の記録媒体にセキュアコンテナを記録してＳＡＭ相互間で配送してもよい。

【０３３０】

第２実施形態

上述した実施形態では、コンテンツプロバイダ１０１からユーザホームネットワーク１０３のＳＡＭ105_1～105_4にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのＳＡＭに配給する場合について説明する。

【０３３１】

図８２は、本実施形態のＥＭＤシステム３００の構成図である。

図８２に示すように、ＥＭＤシステム３００は、コンテンツプロバイダ３０１

、ＥＭＤサービスセンタ３０２、ユーザホームネットワーク３０３、サービスプロバイダ３１０、ペイメントゲートウェイ９０および決済機関９１を有する。

コンテンツプロバイダ３０１、ＥＭＤサービスセンタ３０２、ＳＡＭ305_1～305_4およびサービスプロバイダ３１０は、それぞれ本発明のデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。

コンテンツプロバイダ３０１は、サービスプロバイダ３１０に対してコンテンツデータを供給する点を除いて、前述した第１実施形態のコンテンツプロバイダ１０１と同じである。

また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ１０１およびＳＡＭ505_1～505_4に加えて、サービスプロバイダ３１０に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第１実施形態のＥＭＤサービスセンタ１０２と同じである。

また、ユーザホームネットワーク３０３は、ネットワーク機器360_1およびＡＶ機器360_2～360_4を有している。ネットワーク機器360_1はＳＡＭ305_1およびＣＡモジュール３１１を内蔵しており、ＡＶ機器360_2～360_4はそれぞれＳＡＭ305_2～305_4を内蔵している。

ここで、ＳＡＭ305_1～305_4は、サービスプロバイダ３１０からセキュアコンテナ３０４の配給を受ける点と、コンテンツプロバイダ３０１に加えてサービスプロバイダ３１０についての署名データの検証処理およびＳＰ用購入履歴データ（データ配給装置用購入履歴データ）３０９の作成を行なう点とを除いて、前述した第１実施形態のＳＡＭ105_1～105_4と同じである。

【０３３２】

先ず、ＥＭＤシステム３００の概要について説明する。

ＥＭＤシステム３００では、コンテンツプロバイダ３０１は、自らが提供しようとするコンテンツのコンテンツデータＣの使用許諾条件などの権利内容を示す前述した第１実施形態と同様の権利書(UCP:Usage Control Policy)データ１０６およびコンテンツ鍵データＫｃを、高い信頼性のある権威機関であるＥＭＤサービスセンタ３０２に送信する。権利書データ１０６およびコンテンツ鍵データＫｃは、ＥＭＤサービスセンタ３０２に登録されて権威化（認証）される。

【０３３３】

また、コンテンツプロバイダ３０１は、コンテンツ鍵データＫｃでコンテンツデータＣを暗号化してコンテンツファイルＣＦを生成する。また、コンテンツプロバイダ３０１は、ＥＭＤサービスセンタ３０２から、各コンテンツファイルＣＦについて、それぞれ６か月分のキーファイルＫＦを受信する。

当該キーファイルＫＦ内には、当該キーファイルＫＦの改竄の有無、当該キーファイルＫＦの作成者および送信者の正当性を検証するための署名データが格納されている。

そして、コンテンツプロバイダ３０１は、コンテンツファイルＣＦ、キーファイルＫＦおよび自らの署名データとを格納した図３に示すセキュアコンテナ１０４を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いてあるいはオフラインなどでサービスプロバイダ３１０に供給する。

また、セキュアコンテナ１０４に格納された署名データは、対応するデータの改竄の有無、当該データの作成者および送信者の正当性を検証するために用いられる。

【０３３４】

サービスプロバイダ３１０は、コンテンツプロバイダ３０１からセキュアコンテナ１０４を受け取ると、署名データの検証を行なって、セキュアコンテナ１０４の作成者および送信者の確認する。

次に、サービスプロバイダ３１０は、例えばオフラインで通知されたコンテンツプロバイダ３０１が希望するコンテンツに対しての価格（ＳＲＰ）に、自らが行ったオーサリングなどのサービスに対しての価格を加算した価格を示すプライスタグデータ（ＰＴ：本発明の価格データ）３１２を作成する。

そして、サービスプロバイダ３１０は、セキュアコンテナ１０４から取り出したコンテンツファイルＣＦおよびキーファイルＫＦと、プライスタグデータ３１２と、これらに対しての自らの秘密鍵データ$K_{SP,S}$による署名データとを格納したセキュアコンテナ３０４を作成する。

このとき、キーファイルＫＦは、ライセンス鍵データKD_1～KD_6によって

暗号化されており、サービスプロバイダ３１０は当該ライセンス鍵データKD_1～KD_6を保持していないため、サービスプロバイダ３１０はキーファイルＫＦの中身を見たり、書き換えたりすることはできない。

また、ＥＭＤサービスセンタ３０２は、プライスタグデータ３１２を登録して権威化する。

【０３３５】

サービスプロバイダ３１０は、オンラインおよび／またはオフラインでセキュアコンテナ３０４をユーザホームネットワーク３０３に配給する。

このとき、オフラインの場合には、セキュアコンテナ３０４はＲＯＭ型の記録媒体などに記録されてＳＡＭ305_1～305_4にそのまま供給される。一方、オンラインの場合には、サービスプロバイダ３１０とＣＡモジュール３１１との間で相互認証を行い、セキュアコンテナ３０４をサービスプロバイダ３１０においてセッション鍵データK_{SES}を用いた暗号化して送信し、ＣＡモジュール３１１において受信したセキュアコンテナ３０４をセッション鍵データK_{SES}を用いて復号した後に、ＳＡＭ305_1～305_4に転送する。

この場合に、コンテンツプロバイダ３０１からユーザホームネットワーク３０３にセキュアコンテナ３０４を送信する通信プロコトルとして、デジタル放送であればＭＨＥＧ(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットであればＸＭＬ／ＳＭＩＬ／ＨＴＭＬ(Hyper TextMarkup Language)が用いられ、これらの通信プロトコル内に、セキュアコンテナ３０４が、当該通信プロトコル（符号化方式など）に依存しない形式でトンネリングして埋め込まれる。

従って、通信プロコトルとセキュアコンテナ３０４との間でフォーマットの整合性をとる必要性はなく、セキュアコンテナ３０４のフォーマットを柔軟に設定できる。

【０３３６】

次に、ＳＡＭ305_1～305_4において、セキュアコンテナ３０４内に格納された署名データを検証して、セキュアコンテナ３０４に格納されたコンテンツファイルＣＦおよびキーファイルＫＦの作成者および送信者の正当性を確認する

。そして、ＳＡＭ３０５$_1$～３０５$_4$において、当該正当性が確認されると、ＥＭＤサービスセンタ３０２から配給された対応する期間のライセンス鍵データＫＤ$_1$～ＫＤ$_3$を用いてキーファイルＫＦを復号する。

ＳＡＭ３０５$_1$～３０５$_4$に供給されたセキュアコンテナ３０４は、ネットワーク機器３６０$_1$およびＡＶ機器３６０$_2$～３６０$_4$において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

ＳＡＭ３０５$_1$～３０５$_4$は、上述したセキュアコンテナ３０４の購入・利用の履歴を利用履歴(Usage Log)データ３０８として記録する。

利用履歴データ（履歴データまたは管理装置用履歴データ）３０８は、例えば、ＥＭＤサービスセンタ３０２からの要求に応じて、ユーザホームネットワーク３０３からＥＭＤサービスセンタ３０２に送信される。

また、ＳＡＭ３０５$_1$～３０５$_4$は、コンテンツの購入形態が決定されると、当該購入形態を示す利用制御データ（ＵＣＳ:Usage control state Data）１６６をＥＭＤサービスセンタ３０２に送信する。

【０３３７】

ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、ペイメントゲートウェイ９０を介して銀行などの決済機関９１に決済を行なう。これにより、ユーザホームネットワーク１０３のユーザが支払った金銭が、ＥＭＤサービスセンタ１０２による決済処理によって、コンテンツプロバイダ１０１およびサービスプロバイダ３１０に分配される。

【０３３８】

本実施形態では、ＥＭＤサービスセンタ３０２は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、ＥＭＤサービスセンタ３０２は、中立の立場にある最高の権威機関であるルート認証局９２に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ３０１、サービスプロバイダ

３１０およびＳＡＭ３０５$_1$～３０５$_4$において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、ＥＭＤサービスセンタ３０２の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ３０１の権利書データ１０６、コンテンツ鍵データＫｃおよびサービスプロバイダ３１０のプライスタグデータ３１２を登録して権威化することも、ＥＭＤサービスセンタ３０２の認証機能によるものである。

また、ＥＭＤサービスセンタ３０２は、例えば、ライセンス鍵データＫＤ$_1$～ＫＤ$_6$などの鍵データの管理を行なう鍵データ管理機能を有する。

また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１が登録した権利書データ１０６とＳＡＭ３０５$_1$～ＳＡＭ３０５$_4$から入力した利用履歴データ３０８とサービスプロバイダ３１０が登録したプライスタグデータ３１２とに基づいて、ユーザホームネットワーク３０３のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ３０１およびサービスプロバイダ３１０に分配して支払う権利処理（利益分配）機能を有する。

【０３３９】

以下、コンテンツプロバイダ３０１の各構成要素について詳細に説明する。

〔コンテンツプロバイダ３０１〕

コンテンツプロバイダ３０１は、図３に示すセキュアコンテナ１０４をオンラインあるいはオフラインでサービスプロバイダ３１０に提供する点を除いて、前述した第１実施形態のコンテンツプロバイダ１０１と同じである。

すなわち、コンテンツプロバイダ３０１は、前述した図１７～図１９に示す手順でセキュアコンテナ１０４を作成し、セキュアコンテナ１０４を、コンテンツプロバイダ用商品配送プロトコルに挿入する。

そして、サービスプロバイダ３１０が、ダウンロードを行って、コンテンツプロバイダ用商品配送プロトコルからセキュアコンテナ１０４を取り出す。

【０３４０】

〔サービスプロバイダ３１０〕

サービスプロバイダ３１０は、コンテンツプロバイダ３０１から提供を受けたセキュアコンテナ１０４内のコンテンツファイルＣＦおよびキーファイルＫＦと、自らが生成したプライスタグデータ３１２とを格納したセキュアコンテナ３０４を作成し、ユーザホームネットワーク３０３のネットワーク機器360_1およびＡＶ機器360_2～360_4にセキュアコンテナ３０４をオンラインおよび／またはオフラインで配給する。

サービスプロバイダ３１０によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。

独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、ＣＭ（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【０３４１】

サービスプロバイダ３１０は、コンテンツプロバイダ３０１からセキュアコンテナ１０４の提供を受けると、以下に示す処理を行ってセキュアコンテナ３０４を作成する。

以下、コンテンツプロバイダ３０１から供給を受けたセキュアコンテナ１０４からセキュアコンテナ３０４を作成し、これをユーザホームネットワーク３０３に配給する際のサービスプロバイダ３１０内での処理の流れを図８３を参照しながら説明する。

図８３は、サービスプロバイダ３１０からユーザホームネットワーク３０３にセキュアコンテナ３０４を配給する処理を説明するためのフローチャートである。

＜ステップＳ８３－１＞

サービスプロバイダ３１０は、オンラインおよび／またはオフラインで、コンテンツプロバイダ３０１から図３に示すセキュアコンテナ１０４の供給を受け、これを格納する。

このとき、オンラインの場合には、コンテンツプロバイダ３０１とサービスプ

ロバイダ３１０との間の相互認証によって得られたセッション鍵データK_{SES}を用いて、セキュアコンテナ１０４を復号する。

＜ステップＳ８３－２＞

サービスプロバイダ３１０は、セキュアコンテナ１０４の図３（Ｃ）に示す署名データ$SIG_{1,ESC}$を、ＥＭＤサービスセンタ３０２の公開鍵データ$K_{ESC,P}$を用いて検証し、その正当性が認められた後に、図３（Ｃ）に示す公開鍵証明書データCER_{CP}から公開鍵データ$K_{CP,P}$を取り出す。

次に、サービスプロバイダ３１０は、当該取り出した公開鍵データ$K_{CP,P}$を用いて、セキュアコンテナ１０４の図３（Ａ），（Ｂ）に示す署名データ$SIG_{6,CP}$，$SIG_{7,CP}$の検証、すなわちコンテンツファイルＣＦの作成者および送信者と、キーファイルＫＦの送信者との正当性の検証を行う。

また、サービスプロバイダ３１０は、公開鍵データ$K_{ESC,P}$を用いて、図３（Ｂ）に示すキーファイルＫＦに格納された署名データ$SIG_{K1,ESC}$の検証、すなわちキーファイルＫＦの作成者の正当性の検証を行う。このとき、署名データ$SIG_{K1,ESC}$の検証は、キーファイルＫＦがＥＭＤサービスセンタ３０２に登録されているか否かの検証も兼ねている。

【０３４２】

＜ステップＳ８３－３＞

サービスプロバイダ３１０は、例えばコンテンツプロバイダ３０１からオフラインで通知されたコンテンツプロバイダ３０１が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ３１２を作成する。

また、サービスプロバイダ３１０は、コンテンツファイルＣＦ、キーファイルＫＦおよびプライスタグデータ３１２のハッシュ値をとり、サービスプロバイダ３１０の秘密鍵データ$K_{SP,P}$を用いて、署名データ$SIG_{62,SP}$，$SIG_{63,SP}$，$SIG_{64,SP}$を作成する。

ここで、署名データ$SIG_{62,SP}$はコンテンツファイルＣＦの送信者の正当性を検証するために用いられ、署名データ$SIG_{63,SP}$はキーファイルＫＦの送信者の正当性を検証するために用いられ、署名データ$SIG_{64,SP}$はプライスタグ

データ３１２の作成者および送信者の正当性を検証するために用いられる。

【０３４３】

次に、サービスプロバイダ３１０は、図８４（Ａ）～（Ｄ）に示すように、コンテンツファイルＣＦおよびその署名データ$ＳＩＧ_{6,CP}$，$ＳＩＧ_{62,SP}$と、キーファイルＫＦおよびその署名データ$ＳＩＧ_{7,CP}$，$ＳＩＧ_{63,ESC}$と、プライスタグデータ３１２およびその署名データ$ＳＩＧ_{64,SP}$と、公開鍵証明書データ$ＣＥＲ_{SP}$およびその署名データ$ＳＩＧ_{61,ESC}$と、公開鍵証明書データ$ＣＥＲ_{CP}$およびその署名データ$ＳＩＧ_{1,ESC}$とを格納したセキュアコンテナ３０４を作成し、セキュアコンテナデータベースに格納する。

セキュアコンテナデータベースに格納されたセキュアコンテナ３０４は、例えば、コンテンツＩＤなどを用いてサービスプロバイダ３１０によって一元的に管理される。

なお、図８４（Ａ）は、コンテンツデータＣを伸長するＡＶ圧縮伸長用装置として、ＤＳＰ(Digital Signal Processor)を用いた場合のコンテンツファイルＣＦの構成である。当該ＤＳＰでは、セキュアコンテナ３０４内のＡ／Ｖ伸長用ソフトウェアおよび電子透かし情報モジュールを用いて、セキュアコンテナ１０４内のコンテンツデータＣの伸長および電子透かし情報の埋め込みおよび検出を行う。そのため、コンテンツプロバイダ３０１は任意の圧縮方式および電子透かし情報の埋め込み方式を採用できる。

ＡＶ圧縮伸長用装置としてＡ／Ｖ伸長処理および電子透かし情報の埋め込み・検出処理をハードウェアあるいは予め保持されたソフトウェアを用いて行う場合には、コンテンツファイルＣＦ内にＡ／Ｖ伸長用ソフトウェアおよび電子透かし情報モジュールを格納しなくてもよい。

【０３４４】

＜ステップＳ８３－４＞

サービスプロバイダ３１０は、ユーザホームネットワーク３０３からの要求に応じたセキュアコンテナ３０４をセキュアコンテナデータベースから読み出す。

このとき、セキュアコンテナ３０４は、複数のコンテンツファイルＣＦと、それらにそれぞれ対応した複数のキーファイルＫＦとを格納した複合コンテナであ

ってもよい。例えば、単数のセキュアコンテナ３０４内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルＣＦを単数のセキュアコンテナ３０４に格納してもよい。これらの複数のコンテンツファイルＣＦなどは、ディレクトリー構造でセキュアコンテナ３０４内に格納してもよい。

【０３４５】

また、セキュアコンテナ３０４は、デジタル放送で送信される場合には、ＭＨＥＧ(Multimedia and Hypermedia information coding Experts Group)プロトコルが用いられ、インターネットで送信される場合にはＸＭＬ／ＳＭＩＬ／ＨＴＭＬ(Hyper TextMarkup Language) プロトコルが用いられる。

このとき、セキュアコンテナ３０４内のコンテンツファイルＣＦおよびキーファイルＫＦなどは、ＭＨＥＧおよびＨＴＭＬのプロトコルをトンネリングした符号化方式に依存しない形式で、サービスプロバイダ３１０とユーザホームネットワーク３０３との間で採用される通信プロトコル内の所定の階層に格納される。

【０３４６】

例えば、セキュアコンテナ３０４をデジタル放送で送信する場合には、図８５に示すように、コンテンツファイルＣＦが、ＭＨＥＧオブジェクト(Object)内のＭＨＥＧコンテンツデータとして格納される。

また、ＭＨＥＧオブジェクトは、トランスポート層プロコトルにおいて、動画である場合にはＰＥＳ(Packetized Elementary Stream)－Ｖｉｄｅｏに格納され、音声である場合にはＰＥＳ－Ａｕｄｉｏに格納され、静止画である場合にはＰｒｉｖａｔｅ－Ｄａｔａに格納される。

また、図８６に示すように、キーファイルＫＦ、プライスタグデータ３１２および公開鍵証明書データ$ＣＥＲ_{CP}$，$ＣＥＲ_{SP}$は、トランスポート層プロトコルのTS Packet 内のＥＣＭ(Entitlement Control Message) に格納される。

ここで、コンテンツファイルＣＦ、キーファイルＫＦ、プライスタグデータ３１２および公開鍵証明書データ$ＣＥＲ_{CP}$，$ＣＥＲ_{SP}$は、コンテンツファイルＣＦのヘッダ内のディレクトリ構造データ$ＤＳＤ_1$によって相互間のリンクが確立されている。

【０３４７】

次に、サービスプロバイダ３１０は、セキュアコンテナ３０４を、オフラインおよび／またはオンラインでユーザホームネットワーク３０３に供給する。

サービスプロバイダ３１０は、セキュアコンテナ３０４をオンラインでユーザホームネットワーク３０３のネットワーク機器360_1に配信する場合には、相互認証後に、セッション鍵データK_{SES}を用いてセキュアコンテナ３０４を暗号化した後に、ネットワークを介してネットワーク機器360_1に配信する。

【０３４８】

なお、サービスプロバイダ３１０は、セキュアコンテナ３０４を例えば衛星などを介して放送する場合には、セキュアコンテナ３０４をスクランブル鍵データK_{SCR}を用いて暗号化する。また、スクランブル鍵データK_{SCR}をワーク鍵データK_Wを暗号化し、ワーク鍵データK_Wをマスタ鍵データK_Mを用いて暗号化する。

そして、サービスプロバイダ３１０は、セキュアコンテナ３０４と共に、スクランブル鍵データK_{SCR}およびワーク鍵データK_Wを、衛星を介してユーザホームネットワーク３０３に送信する。

また、例えば、マスタ鍵データK_Mを、ＩＣカードなどに記憶してオフラインでユーザホームネットワーク３０３に配給する。

【０３４９】

また、サービスプロバイダ３１０は、ユーザホームネットワーク３０３から、当該サービスプロバイダ３１０が配給したコンテンツデータＣに関してのＳＰ用購入履歴データ３０９を受信すると、これを格納する。

サービスプロバイダ３１０は、将来のサービス内容を決定する際に、ＳＰ用購入履歴データ３０９を参照する。また、サービスプロバイダ３１０は、ＳＰ用購入履歴データ３０９に基づいて、当該ＳＰ用購入履歴データ３０９を送信したＳＡＭ305_1～305_4のユーザの嗜好を分析してユーザ嗜好フィルタデータ９００を生成し、これをユーザホームネットワーク３０３のＣＡモジュール３１１に送信する。

【０３５０】

また、サービスプロバイダ３１０の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、ＥＭＤサービスセンタ３０２に登録処理を行い、グローバルユニークな識別子ＳＰ＿ＩＤを得ている。

【０３５１】

また、サービスプロバイダ３１０は、ＥＭＤサービスセンタ３０２にプライスタグデータ３１２を登録して権威化してる。

【０３５２】

〔ＥＭＤサービスセンタ３０２〕

ＥＭＤサービスセンタ３０２は、前述したように、認証局（ＣＡ:Certificate Authority）、鍵管理(Key Management)局および権利処理(Rights Clearing) 局としての役割を果たす。

図８７は、ＥＭＤサービスセンタ３０２の主な機能を示す図である。

図８７に示すように、ＥＭＤサービスセンタ３０２は、主に、ライセンス鍵データをコンテンツプロバイダ３０１およびＳＡＭ305_1～305_4に供給する処理と、公開鍵証明書データCER_{CP}，CER_{SP}，CER_{SAM1}～CER_{SAM4}の発行処理と、キーファイルＫＦの発行処理、利用履歴データ３０８に基づいた決済処理（利益分配処理）とを行う。

ここで、ライセンス鍵データの供給処理と、公開鍵証明書データCER_{CP}，CER_{SAM1}～CER_{SAM4}の発行処理と、キーファイルＫＦの生成処理とは、第１実施形態のＥＭＤサービスセンタ１０２と同じである。

【０３５３】

ＥＭＤサービスセンタ３０２は、ＥＭＤサービスセンタ１０２とは異なり、さらにサービスプロバイダ３１０の公開鍵証明書データCER_{SP}の発行処理を行う。

また、ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、ＳＡＭ305_1～305_4におけるコンテンツデータＣの購入によって支払われた利益をコンテンツプロバイダ３０１およびサービスプロバイダ３１０の関係者に分配する利益分配処理を行う。

ここで、利用履歴データ３０８の内容は、例えば図２１に示される。

【０３５４】

また、ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、当該利用履歴データ３０８を送信したＳＡＭ305_1～305_4のユーザの嗜好に応じたコンテンツデータＣを選択するためのユーザ嗜好フィルタデータ９０３を生成し、ユーザ嗜好フィルタデータ９０３をＳＡＭ管理部１４９を介して、当該利用履歴データ３０８を送信したＳＡＭ305_1～305_4に送信する。

【０３５５】

〔ユーザホームネットワーク３０３〕

ユーザホームネットワーク３０３は、図８２に示すように、ネットワーク機器360_1およびＡ／Ｖ機器360_2～360_4を有している。

ネットワーク機器360_1は、ＣＡモジュール３１１およびＳＡＭ305_1を内蔵している。また、ＡＶ機器360_2～360_4は、それぞれＳＡＭ305_2～305_4を内蔵している。

ＳＡＭ305_1～305_4の相互間は、例えば、１３９４シリアルインタフェースバスなどのバス１９１を介して接続されている。

なお、ＡＶ機器360_2～360_4は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス１９１を介してネットワーク機器360_1のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク３０３は、ネットワーク機能を有していないＡＶ機器のみを有していてもよい。

【０３５６】

以下、ネットワーク機器360_1について説明する。

図８８は、ネットワーク機器360_1の構成図である。

図８８に示すように、ネットワーク機器360_1は、通信モジュール１６２、ＣＡモジュール３１１、復号モジュール９０５、ＳＡＭ305_1、ＡＶ圧縮・伸長用ＳＡＭ１６３、操作部１６５、ダウンロードメモリ１６７、再生モジュール１６９、外部メモリ２０１およびホストＣＰＵ８１０を有する。

図８８において、図２２と同一符号を付した構成要素は、第１実施形態で説明

した同一符号の構成要素と同じである。

【０３５７】

通信モジュール１６２は、サービスプロバイダ３１０との間の通信処理を行なう。

具体的には、通信モジュール１６２は、サービスプロバイダ３１０から衛星放送などで受信したセキュアコンテナ３０４を復号モジュール９０５に出力する。また、通信モジュール１６２は、サービスプロバイダ３１０から電話回線などを介して受信したユーザ嗜好フィルタデータ９００をＣＡモジュール３１１に出力すると共に、ＣＡモジュール３１１から入力したＳＰ用購入履歴データ３０９を電話回線などを介してサービスプロバイダ３１０に送信する。

【０３５８】

図８９は、ＣＡモジュール３１１および復号モジュール９０５の機能ブロック図である。

図８９に示すように、ＣＡモジュール３１１は、相互認証部９０６、記憶部９０７、暗号化・復号部９０８およびＳＰ用購入履歴データ生成部９０９を有する。

相互認証部９０６は、ＣＡモジュール３１１とサービスプロバイダ３１０との間で電話回線を介してデータを送受信する際に、サービスプロバイダ３１０との間で相互認証を行ってセッション鍵データK_{SES}を生成し、これを暗号化・復号部９０８に出力する。

【０３５９】

記憶部９０７は、例えば、サービスプロバイダ３１０とユーザとの間で契約が成立した後に、サービスプロバイダ３１０からＩＣカード９１２などを用いてオフラインで供給されたマスタ鍵データK_Mを記憶する。

【０３６０】

暗号化・復号部９０８は、復号モジュール９０５の復号部９１０からそれぞれ暗号化されたスクランブル鍵データK_{SCR}およびワーク鍵データK_Wを入力し、記憶部９０７から読み出したマスタ鍵データK_Mを用いてワーク鍵データK_Wを復号する。そして、暗号化・復号部９０８は、当該復号したワーク鍵データK_W

を用いてスクランブル鍵データK_{SCR}を復号し、当該復号したスクランブル鍵データK_{SCR}を復号部９１０に出力する。

また、暗号化・復号部９０８は、電話回線などを介して通信モジュール１６２がサービスプロバイダ３１０から受信したユーザ嗜好フィルタデータ９００を、相互認証部９０６からのセッション鍵データK_{SES}を用いて復号して復号モジュール９０５のセキュアコンテナ選択部９１１に出力する。

また、暗号化・復号部９０８は、ＳＰ用購入履歴データ生成部９０９から入力したＳＰ用購入履歴データ３０９を、相互認証部９０６からのセッション鍵データK_{SES}を用いて復号して通信モジュール１６２を介してサービスプロバイダ３１０に送信する。

【０３６１】

ＳＰ用購入履歴データ生成部９０９は、図８８に示す購入・利用形態決定操作部１６５を用いてユーザによるコンテンツデータＣの購入操作に応じた操作信号Ｓ１６５、またはＳＡＭ305_1からの利用制御データ１６６に基づいて、サービスプロバイダ３１０に固有のコンテンツデータＣの購入履歴を示すＳＰ用購入履歴データ３０９を生成し、これを暗号化・復号部９０８に出力する。

ＳＰ用購入履歴データ３０９は、例えば、サービスプロバイダ３１０が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃）、契約（更新）情報および購入履歴情報などを含む。

【０３６２】

なお、ＣＡモジュール３１１は、サービスプロバイダ３１０が課金機能を有している場合には、サービスプロバイダ３１０の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、ＣＡモジュール３１１は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ３１０に送信する。

【０３６３】

復号モジュール９０５は、復号部９１０およびセキュアコンテナ選択部９１１を有する。

復号部９１０は、通信モジュール１６２から、それぞれ暗号化されたセキュア

コンテナ３０４、スクランブル鍵データK_{SCR}およびワーク鍵データK_Wを入力する。

そして、復号部９１０は、暗号化されたスクランブル鍵データK_{SCR}およびワーク鍵データK_WをＣＡモジュール３１１の暗号化・復号部９０８に出力し、暗号化・復号部９０８から復号されたスクランブル鍵データK_{SCR}を入力する。

そして、復号部９１０は、暗号化されたセキュアコンテナ３０４を、スクランブル鍵データK_{SCR}を用いて復号した後に、セキュアコンテナ選択部９１１に出力する。

【０３６４】

なお、セキュアコンテナ３０４が、MPEG2 Transport Stream 方式でサービスプロバイダ３１０から送信される場合には、例えば、復号部９１０は、TS Packet 内のＥＣＭ(Entitlement Control Message) からスクランブル鍵データK_{SCR}を取り出し、ＥＭＭ(Entitlement Management Message)からワーク鍵データK_Wを取り出す。

ＥＣＭには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、ＥＭＭは、その他に、ユーザ（視聴者）毎に異なる個別試聴契約情報などが含まれている。

【０３６５】

セキュアコンテナ選択部９１１は、復号部９１０から入力したセキュアコンテナ３０４を、ＣＡモジュール３１１から入力したユーザ嗜好フィルタデータ９００を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ３０４を選択して$SAM305_1$に出力する。

【０３６６】

次に、$SAM305_1$について説明する。

なお、$SAM305_1$は、サービスプロバイダ３１０についての署名検証処理を行なうなど、コンテンツプロバイダ３０１に加えてサービスプロバイダ３１０に関しての処理を行う点を除いて、図２２～図７２などを用いて前述した第１実施形態の$SAM105_1$と基本的に行なう機能および構造を有している。
している。

ＳＡＭ３０５$_1$～３０５$_4$は、コンテンツ単位の課金処理を行うモジュールであり、ＥＭＤサービスセンタ３０２との間で通信を行う。

【０３６７】

また、図６３に示す構成はユーザホームネットワーク３０３内の機器においても適用可能である。また、図６８～図７９を用いて説明した権利処理用のＳＡＭ、メディアＳＡＭ１３３、ＡＶ圧縮・伸長用ＳＡＭ１６３およびメディア・ドラブＳＡＭ２６０の構成は、ユーザホームネットワーク３０３内の機器で用いられる各種のＳＡＭにも適用される。

また、ＳＡＭ３０５$_2$～３０５$_4$は、ＳＡＭ３０５$_1$と基本的に同じ機能を有

【０３６８】

以下、ＳＡＭ３０５$_1$の機能について詳細に説明する。

図９０は、ＳＡＭ３０５$_1$の機能の構成図である。

なお、図９０には、サービスプロバイダ３１０からセキュアコンテナ３０４を入力する際の処理に関連するデータの流れが示されている。

図９０に示すように、ＳＡＭ３０５$_1$は、相互認証部１７０、暗号化・復号部１７１，１７２，１７３、ダウンロードメモリ管理部１８２、ＡＶ圧縮・伸長用ＳＡＭ管理部１８４、ＥＭＤサービスセンタ管理部１８５、利用監視部１８６、ＳＡＭ管理部１９０、記憶部１９２、メディアＳＡＭ管理部１９７、作業用メモリ２００、サービスプロバイダ管理部５８０、課金処理部５８７、署名処理部５８９、外部メモリ管理部８１１およびＣＰＵ１１００を有する。

なお、図９０に示すＳＡＭ３０５$_1$の所定の機能は、ＳＡＭ１０５$_1$の場合と同様に、ＣＰＵにおいて秘密プログラムを実行することによって実現される。

図９０において、図３０等と同じ符号を付した機能ブロックは、第１実施形態で説明した同一符号の機能ブロックと同じである。

【０３６９】

また、図８８に示す外部メモリ２０１には、第１実施形態で説明した処理および後述する処理を経て、利用履歴データ３０８およびＳＡＭ登録リストが記憶される。

また、作業用メモリ２００には、図９１に示すように、コンテンツ鍵データＫ

c、権利書データ（ＵＣＰ）１０６、記憶部１９２のロック鍵データK_{LOC}、コンテンツプロバイダ３０１の公開鍵証明書データCER_{CP}、サービスプロバイダ３１０の公開鍵証明書データCER_{SP}、利用制御データ（ＵＣＳ）３６６、ＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3およびプライスタグデータ３１２などが記憶される。

【０３７０】

以下、$SAM305_1$の機能ブロックのうち、図９０において新たに符号を付した機能ブロックについて説明する。

署名処理部５８９は、記憶部１９２あるいは作業用メモリ２００から読み出したＥＭＤサービスセンタ３０２の公開鍵データ$K_{ESC,P}$、コンテンツプロバイダ３０１の公開鍵データ$K_{cp,p}$およびサービスプロバイダ３１０の公開鍵データ$K_{SP,P}$を用いて、セキュアコンテナ３０４内の署名データの検証を行なう。

【０３７１】

課金処理部５８７は、図９２に示すように、ユーザによる購入形態決定操作に応じた内部割り込みＳ８１０をＣＰＵ１１００がホストＣＰＵ８１０から受けると、ＣＰＵ１１００からの制御によって、作業用メモリ２００から読み出されたプライスタグデータ３１２に基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。

なお、プライスタグデータ３１２は、ユーザがコンテンツデータの購入形態等を決定する際に、所定の出力手段を介して$SAM305_1$の外部に出力され、コンテンツデータの販売価格をユーザに表示等するために用いられる。

課金処理部５８７による課金処理は、利用監視部１８６の監視の下、権利書データ１０６が示す使用許諾条件などの権利内容および利用制御データ１６６に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【０３７２】

また、課金処理部５８７は、課金処理において、利用履歴データ３０８を生成あるいは更新し、これを外部メモリ管理部８１１を介して外部メモリ２０１に書き込む。

ここで、利用履歴データ３０８は、第１実施形態の利用履歴データ１０８と同様に、ＥＭＤサービスセンタ３０２において、セキュアコンテナ３０４に関連したラインセンス料の支払いを決定する際に用いられる。

【０３７３】

また、課金処理部５８７は、ユーザによる購入形態決定操作に応じたＣＰＵ１００の制御に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御（UCS: Usage Control Status ）データ１６６を生成し、これを作業用メモリ２００に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御データ１６６は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御データ１６６には、コンテンツのＩＤ、購入形態、買い切り価格、当該コンテンツの購入が行なわれたＳＡＭのＳＡＭ＿ＩＤ，購入を行なったユーザのＵＳＥＲ＿ＩＤなどが記述されている。

【０３７４】

なお、決定された購入形態が再生課金である場合には、例えば、ＳＡＭ３０５$_1$からサービスプロバイダ３１０に利用制御データ１６６をリアルタイムに送信し、サービスプロバイダ３１０がＥＭＤサービスセンタ３０２に、利用履歴データ３０８をＳＡＭ１０５$_1$に取りに行くことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御データ１６６が、サービスプロバイダ３１０およびＥＭＤサービスセンタ３０２にリアルタイムに送信される。

【０３７５】

また、ＳＡＭ３０５$_1$では、図９０に示すように、ＥＭＤサービスセンタ管理部１８５を介してＥＭＤサービスセンタ３０２から受信したユーザ嗜好フィルタデータ９０３が、サービスプロバイダ管理部５８０に出力される。そして、サー

ビスプロバイダ管理部５８０において、図８８に示す復号モジュール９０５から入力したセキュアコンテナ３０４のうち、ユーザ嗜好フィルタデータ９０３に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ３０４が選択され、当該選択されたセキュアコンテナ３０４がダウンロードメモリ管理部１８２に出力される。これにより、$SAM305_1$ において、当該$SAM305_1$のユーザが契約している全てのサービスプロバイダ３１０を対象として、当該ユーザによるコンテンツデータＣの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータＣの選択処理が可能になる。

【０３７６】

以下、$SAM305_1$ 内での処理の流れを説明する。

＜ライセンス鍵データの受信時の処理＞

ＥＭＤサービスセンタ３０２から受信したライセンス鍵データKD_1～KD_3を記憶部１９２に格納する際の$SAM305_1$ 内での処理の流れは、図３５を用いて前述した第１実施形態の$SAM105_1$ の場合と同様である。

【０３７７】

＜セキュアコンテナ３０４をサービスプロバイダ３１０から入力した時の処理＞

次に、セキュアコンテナ３０４をサービスプロバイダ３１０から入力する際の$SAM305_1$ 内での処理の流れを図９３を参照しながら説明する。

なお、以下に示す例では、$SAM105_1$ において、セキュアコンテナ１０４を入力したときに種々の署名データの検証を行う場合を例示するが、セキュアコンテナ１０４の入力したときには当該署名データの検証を行わずに、購入・利用形態を決定するときに当該署名データの検証を行うようにしてもよい。

【０３７８】

ステップＳ９３－０：図９０に示す$SAM305_1$ のＣＰＵ１１００は、ホストＣＰＵ８１０から、セキュアコンテナの入力処理を行うことを指示する内部割り込みＳ８１０を受ける。

ステップＳ９３－１：図９０に示す$SAM305_1$ の相互認証部１７０とサービスプロバイダ３１０との間で相互認証を行なう。

ステップＳ９３－２：ＳＡＭ３０５$_1$の相互認証部１７０とダウンロードメモリ１６７のメディアＳＡＭ１６７ａとの間で相互認証を行なう。

【０３７９】

ステップＳ９３－３：サービスプロバイダ３１０から受信したセキュアコンテナ３０４を、ダウンロードメモリ１６７に書き込む。

このとき、ステップＳ９３－２で得られたセッション鍵データを用いて、相互認証部１７０におけるセキュアコンテナ３０４の暗号化と、メディアＳＡＭ１６７ａにおけるセキュアコンテナ３０４の復号とを行なう。

ステップＳ９３－４：ＳＡＭ３０５$_1$は、ステップＳ９３－１で得られたセッション鍵データを用いて、セキュアコンテナ３０４の復号を行なう。

【０３８０】

ステップＳ９３－５：署名処理部５８９は、図８４（Ｄ）に示す署名データＳＩＧ$_{61,ESC}$の検証を行なった後に、図８４（Ｄ）に示す公開鍵証明書データＣＥＲ$_{SP}$内に格納されたサービスプロバイダ３１０の公開鍵データＫ$_{SP,P}$を用いて、署名データＳＩＧ$_{62,SP}$，ＳＩＧ$_{63,SP}$，ＳＩＧ$_{64,SP}$の正当性を検証する。

このとき、署名データＳＩＧ$_{62,SP}$が正当であると検証されたときに、コンテンツファイルＣＦの送信者の正当性が確認される。署名データＳＩＧ$_{63,SP}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。署名データＳＩＧ$_{64,SP}$が正当であると検証されたときに、プライスタグデータ３１２の作成者および送信者の正当性が確認される。

【０３８１】

ステップＳ９３－６：署名処理部５８９は、図８４（Ｄ）に示す署名データＳＩＧ$_{1,ESC}$の検証を行なった後に、図８４（Ｃ）に示す公開鍵証明書データＣＥＲ$_{CP}$内に格納されたコンテンツプロバイダ３０１の公開鍵データＫ$_{CP,P}$を用いて、署名データＳＩＧ$_{6,CP}$，ＳＩＧ$_{7,CP}$の正当性を検証する。

このとき、署名データＳＩＧ$_{6,CP}$が正当であると検証されたときに、コンテンツファイルＣＦの作成者および送信者の正当性が確認される。

また、署名データＳＩＧ$_{7,CP}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。

【０３８２】

ステップＳ９３－７：署名処理部５８９は、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて、図８４（Ｂ）に示すキーファイルＫＦ内の署名データ$SIG_{K1,ESC}$の正当性、すなわちキーファイルＫＦの作成者の正当性およびキーファイルＫＦがＥＭＤサービスセンタ１０２に登録されているか否かの検証を行う。

【０３８３】

ステップＳ９３－８：暗号化・復号部１７２は、記憶部１９２から読み出した対応する期間のライセンス鍵データKD_1～KD_3を用いて、図８４（Ｂ）に示すキーファイルＫＦ内のコンテンツ鍵データＫｃ、権利書データ１０６およびＳＡＭプログラム・ダウンロード・コンテナSDC_1～SDC_3を復号し、これらを作業用メモリ２００に書き込む。

【０３８４】

ステップＳ９３－９：ＣＰＵ１１００は、上述したセキュアコンテナの入力処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述したセキュアコンテナの入力処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０３８５】

＜ダウンロードしたセキュアコンテナの購入形態決定処理＞

ダウンロードしたセキュアコンテナの購入形態決定処理は、基本的に、第１実施形態において、図３８を用いて前述した$SAM105_1$の場合と同じである。

当該購入形態決定処理により、後述する図９７（Ｃ）に示すキーファイルKF_1が作業用メモリ２００およびダウンロードメモリ管理部１８２を介してダウンロードメモリ１６７に記憶される。

【０３８６】

＜コンテンツデータの再生処理＞

ダウンロードメモリ１６７に記憶されている購入形態が既に決定されたコンテンツデータＣの再生処理は、基本的に、第１実施形態において、図４０を用いて

説明したＳＡＭ１０５$_1$の処理と同じである。

【０３８７】

＜一の機器の利用制御データ（ＵＳＣ）１６６を使用して他の機器で再購入を行う場合の処理＞

先ず、図９４に示すように、例えば、ネットワーク機器３６０$_1$のダウンロードメモリ１６７にダウンロードされたコンテンツファイルＣＦの購入形態を前述したように決定した後に、当該コンテンツファイルＣＦを格納した新たなセキュアコンテナ３０４ｘを生成し、バス１９１を介して、ＡＶ機器３６０$_2$のＳＡＭ３０５$_2$にセキュアコンテナ３０４ｘを転送するまでのＳＡＭ１０５$_1$内での処理の流れを図９５および図９６を参照しながら説明する。

【０３８８】

図９６は、当該処理のフローチャートである。

図９６に示す処理を行う前提として、前述した購入処理によって、ＳＡＭ３０５$_1$の作業用メモリ２００には図９７（Ｃ）に示すキーファイルKF_1およびそのハッシュ値H_{K1}が記憶されている。

ステップＳ９６－１：ユーザは図８８および図９４に示すに操作部１６５を操作し、購入形態を既に決定したセキュアコンテナをＳＡＭ３０５$_2$に転送することを示す内部割り込みＳ８１０がホストＣＰＵ８１０から図９５に示すＣＰＵ１１００に出される。

課金処理部５８７は、ＣＰＵ１１００の制御に基づいて、決定された購入形態に応じて、外部メモリ２０１に記憶されている利用履歴データ３０８を更新する。

【０３８９】

ステップＳ９６－２：ＳＡＭ３０５$_1$は、第１実施形態で前述したＳＡＭ登録リストを検証し、セキュアコンテナの転送先のＳＡＭ３０５$_2$が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ９６－３以降の処理を行う。

また、ＳＡＭ１０５$_1$は、ＳＡＭ１０５$_2$がホームネットワーク内のＳＡＭであるか否かの検証も行う。

【０３９０】

ステップＳ９６－３：相互認証部１７０は、ＳＡＭ３０５$_2$との間で相互認証を行って得たセッション鍵データK_{SES}を共有する。

【０３９１】

ステップＳ９６－４：ＳＡＭ管理部１９０は、ダウンロードメモリ２１１から図８４（Ａ）に示すコンテンツファイルＣＦおよび署名データ$SIG_{6,CP}$，$SIG_{62,SP}$を読み出し、これについてのＳＡＭ１０５$_1$の秘密鍵データK_{SAM1}を用いた署名データ$SIG_{41,SAM1}$を署名処理部１８９に作成させる。

【０３９２】

ステップＳ９６－５：ＳＡＭ管理部１９０は、ダウンロードメモリ２１１から図８４（Ｂ）に示すキーファイルＫＦおよび署名データ$SIG_{7,CP}$，$SIG_{63,SP}$を読み出し、これについてのＳＡＭ３０５$_1$の秘密鍵データK_{SAM1}を用いた署名データ$SIG_{42,SAM1}$を署名処理部５８９に作成させる。

【０３９３】

ステップＳ９６－６：ＳＡＭ管理部１９０は、図９７に示すセキュアコンテナ３０４ｘを作成する。

ステップＳ９６－７：暗号化・復号部１７１において、ステップＳ９６－３で得たセッション鍵データK_{SES}を用いて、図９７に示すセキュアコンテナ３０４ｘが暗号化される。

【０３９４】

ステップＳ９６－８：ＳＡＭ管理部１９０は、セキュアコンテナ３０４ｘを図９４に示すＡＶ機器３６０$_2$のＳＡＭ３０５$_2$に出力する。

このとき、ＳＡＭ３０５$_1$とＳＡＭ３０５$_2$との間の相互認証と並行して、ＩＥＥＥ１３９４シリアルバスであるバス１９１の相互認証が行われる。

【０３９５】

ステップＳ９６－９：ＣＰＵ１１００は、上述したセキュアコンテナの転送処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述したセキュアコンテナの転送処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８

１０がポーリングによって当該フラグを読んでもよい。

【０３９６】

以下、図９４に示すように、ＳＡＭ３０５$_1$から入力した図９７に示すセキュアコンテナ３０４ｘを、ＲＡＭ型などの記録媒体（メディア）１３０$_4$に書き込む際のＳＡＭ３０５$_2$内での処理の流れを図９８，図９９および図１００を参照して説明する。

図９９および図１００は、当該処理を示すフローチャートである。

ここで、ＲＡＭ型の記録媒体１３０$_4$は、例えば、セキュアでないＲＡＭ領域１３４、メディアＳＡＭ１３３およびセキュアＲＡＭ領域１３２を有している。

【０３９７】

ステップＳ９９－０：図９８に示すＳＡＭ３０５$_2$のＣＰＵ１１００は、ホストＣＰＵ８１０から、入力したセキュアコンテナを購入形態を決定した後に記録媒体に記録することを指示する内部割り込みＳ８１０を受ける。

【０３９８】

ステップＳ９９－１：ＳＡＭ３０５$_2$は、ＳＡＭ登録リストを検証し、セキュアコンテナの転送元のＳＡＭ３０５$_1$が正規に登録されているＳＡＭであるか否かを検証し、正規に登録されていると判断した場合にステップＳ９９－２以降の処理を行う。

また、ＳＡＭ３０５$_2$は、ＳＡＭ３０５$_1$がホームネットワーク内のＳＡＭであるか否かの検証も行う。

【０３９９】

ステップＳ９９－２：前述したステップＳ９９－４－２に対応する処理として、ＳＡＭ３０５$_2$は、ＳＡＭ３０５$_1$との間で相互認証を行って得たセッション鍵データK_{SES}を共有する。

ステップＳ９９－３：ＳＡＭ３０５$_2$のＳＡＭ管理部１９０は、図９４に示すように、ネットワーク機器３６０$_1$のＳＡＭ３０５$_1$からセキュアコンテナ３０４ｘを入力する。

ステップＳ９９－４：暗号化・復号部１７１は、ステップＳ９９－２で共有したセッション鍵データK_{SES}を用いて、ＳＡＭ管理部１９０を介して入力したセ

キュアコンテナ３０４ｘを復号する。

【０４００】

ステップＳ９９－５：セッション鍵データK_{SES}を用いて復号されたセキュアコンテナ３０４ｘ内のコンテンツファイルＣＦが、図９４に示すメディア・ドラブＳＡＭ２６０におけるセクタライズ(Sectorize)、セクタヘッダの付加処理、スクランブル処理、ＥＣＣエンコード処理、変調処理および同期処理を経て、ＲＡＭ型の記録媒体130_4のＲＡＭ領域１３４に記録される。

【０４０１】

ステップＳ９９－６：セッション鍵データK_{SES}を用いて復号されたセキュアコンテナ３０４ｘ内の署名データ$SIG_{6,CP}$，$SIG_{62,SP}$，$SIG_{41,SAM1}$と、キーファイルＫＦおよびその署名データ$SIG_{7,CP}$，，$SIG_{63,SP}$，$SIG_{42,SAM1}$と、キーファイルKF_1およびそのハッシュ値H_{K1}と、公開鍵署名データCER_{SP}およびその署名データ$SIG_{61,ESC}$と、公開鍵署名データCER_{CP}およびその署名データ$SIG_{1,ESC}$と、公開鍵署名データCER_{SAM1}およびその署名データ$SIG_{22,ESC}$とが、作業用メモリ２００に書き込まれる。

【０４０２】

ステップＳ９９－７：署名処理部５８９において、作業用メモリ２００から読み出された署名データ$SIG_{61,ESC}$，$SIG_{1,ESC}$，$SIG_{22,ESC}$が、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて検証され、公開鍵証明書データCER_{SP}，CER_{CP}，CER_{SAM1}の正当性が確認される。

そして、署名処理部５８９において、公開鍵証明書データCER_{CP}に格納された公開鍵データ$K_{CP,P}$を用いて、署名データ$SIG_{6,CP}$の正当性が検証され、コンテンツファイルＣＦの作成者の正当性が確認される。署名処理部５８９において、公開鍵証明書データCER_{SP}に格納された公開鍵データ$K_{SP,P}$を用いて、署名データ$SIG_{62,CP}$の正当性が検証され、コンテンツファイルＣＦの送信者の正当性が確認される。また、署名処理部１８９において、公開鍵証明書データCER_{SAM1}に格納された公開鍵データ$K_{SAM1,P}$を用いて、署名データ$SIG_{41,SAM1}$の正当性が検証され、コンテンツファイルＣＦの送信者の正当性が確認される。

【０４０３】

ステップＳ９９－８：署名処理部５８９において、公開鍵証明書データＣＥＲ$_{CP}$，ＣＥＲ$_{SP}$，ＣＥＲ$_{SAM1}$に格納された公開鍵データ$K_{CP,P}$，$K_{SP,P}$，$K_{SAM1,P}$を用いて、作業用メモリ２００に記憶されている署名データＳＩＧ$_{7,CP}$，ＳＩＧ$_{63,SP}$，ＳＩＧ$_{42,SAM1}$の正当性を検証する。そして、署名データＳＩＧ$_{7,CP}$，ＳＩＧ$_{63,SP}$，ＳＩＧ$_{42,SAM1}$が正当であると検証されたときに、キーファイルＫＦの送信者の正当性が確認される。

【０４０４】

ステップＳ９９－９：署名処理部５８９において、記憶部１９２から読み出した公開鍵データ$K_{ESC,P}$を用いて、図９７（Ｂ）のキーファイルＫＦに格納されが署名データＳＩＧ$_{K1,ESC}$の検証が行われる。そして、署名データＳＩＧ$_{K1,ESC}$が正当であると検証されたときに、キーファイルＫＦの作成者の正当性が確認される。

【０４０５】

ステップＳ９９－１０：署名処理部１８９は、ハッシュ値H_{K1}の正当性を検証し、キーファイルKF_1の作成者および送信者の正当性を確認する。

なお、当該例では、キーファイルKF_1の作成者と送信元とが同じ場合を述べたが、キーファイルKF_1の作成者と送信元とが異なる場合には、キーファイルKF_1に対して作成者の署名データと送信者と署名データとが作成され、署名処理部１８９において、双方の署名データの正当性が検証される。

【０４０６】

ステップＳ９９－１１：利用監視部１８６は、ステップＳ９９－１０で復号されたキーファイルKF_1に格納された利用制御データ１６６を用いて、以後のコンテンツデータＣの購入・利用形態を制御する。

【０４０７】

ステップＳ９９－１２：ユーザは、購入・利用形態決定操作部１６５を操作して購入形態を決定し、当該操作に応じた操作信号Ｓ１６５が、課金処理部５８７に出力される。

ステップＳ９９－１３：課金処理部５８７は、操作信号Ｓ１６５に基づいて、

外部メモリ２０１に記憶されている利用履歴データ３０８を更新する。

また、課金処理部５８７は、コンテンツデータの購入形態が決定される度に、当該決定された購入形態に応じて利用制御データ１６６を更新する。

【０４０８】

ステップＳ９９－１４：暗号化・復号部１７３は、記憶部１９２から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED}および購入者鍵データK_{PIN}を順に用いて、ステップＳ９９－１２で生成された利用制御データ１６６を暗号化してメディア・ドライブＳＡＭ管理部８５５に出力する。

ステップＳ９９－１５：メディア・ドライブＳＡＭ管理部８５５は、新たな利用制御データ１６６を格納したキーファイルKF_1を、セクタライズ処理、セクタヘッダの付加処理、スクランブル処理、ＥＣＣエンコード処理、変調処理および同期処理を経て、ＲＡＭ型の記録媒体130_4のセキュアＲＡＭ領域１３２に記録する。

ステップＳ９９－１６：キーファイルＫＦが作業用メモリ２００から読み出され、メディア・ドライブＳＡＭ管理部８５５を介して、図９４に示すメディア・ドラブＳＡＭ２６０によってＲＡＭ型の記録媒体130_4のセキュアＲＡＭ領域１３２に書き込まれる。

【０４０９】

ステップＳ９９－１７：ＣＰＵ１１００は、上述した処理が適切に行われたか否かを、外部割り込みでホストＣＰＵ８１０に通知する。

なお、ＣＰＵ１１００は、上述した処理が適切に行われたか否かを示すＳＡＭステータスレジスタのフラグを設定し、ホストＣＰＵ８１０がポーリングによって当該フラグを読んでもよい。

【０４１０】

なお、$SAM305_1$におけるＲＯＭ型の記録媒体のコンテンツデータの購入形態決定処理、ＲＯＭ型の記録媒体のコンテンツデータの購入形態を決定した後にＲＡＭ型の記録媒体に書き込む場合の処理は、サービスプロバイダ３１０において秘密鍵データ$K_{SP,P}$を用いて付けられた署名データSIG_{SP}の検証処理を行う点を除いて、前述した第１実施形態の$SAM105_1$における処理と同じであ

る。

また、ＳＡＭ３０５$_1$の実現方法も、前述した第１実施形態で説明したＳＡＭ１０５$_1$の実現方法と同じである。

また、ユーザホームネットワーク３０３に用いられる機器においても、第１実施形態で説明した図６３に示す構成は同様に適用される。また、この場合に、ＳＡＭ３０５$_1$、ＡＶ圧縮・伸長用ＳＡＭ１６３、メディア・ドラブＳＡＭ２６０およびメディアＳＡＭ１３３の回路モジュールとして、図６４～図７９を用いて説明した構成が同様に適用される。

また、図６２を用いて説明したセキュア機能も、コンテンツプロバイダ１０１がサービスプロバイダ３１０に置き換える点を除いて、ＥＭＤシステム３００でも同様に適用される。

【０４１１】

以下、ユーザホームネットワーク３０３における各種の機器の接続形態等を再び説明する。

図１０１は、ユーザホームネットワーク３０３における機器の接続形態の一例を説明するための図である。

ここでは、図１０１に示すように、ユーザホームネットワーク３０３内でネットワーク機器３６０$_1$，ＡＶ機器３６０$_2$，３６０$_3$がＩＥＥＥ１３９４シリアルバス１９１を介して接続されている場合を説明する。

ネットワーク機器３６０$_1$は、外部メモリ２０１、ＳＡＭ３０５$_1$、ＣＡモジュール３１１、ＡＶ圧縮・伸長用ＳＡＭ１６３およびダウンロードメモリ１６７を有する。

ＣＡモジュール３１１は、公衆回線などのネットワークを介して、サービスプロバイダ３１０と通信を行う。

また、ＳＡＭ３０５$_1$は、公衆回線などのネットワークを介して、ＥＭＤサービスセンタ３０２と通信を行う。

ダウンロードメモリ１６７としては、メディアＳＡＭ１６７ａを備えたメモリスティック、あるいはＨＤＤなどが用いられる。ダウンロードメモリ１６７には、サービスプロバイダ３１０からダウンロードしたセキュアコンテナ３０４など

が記憶される。

各機器には、ＡＴＲＡＣ３やＭＰＥＧなどの各種の圧縮・伸長方式にそれぞれ対応した複数のＡＶ圧縮・伸長用ＳＡＭ１６３が内蔵されている。

ＳＡＭ３０５$_1$は、接触方式あるいは非接触方式のＩＣカード１１４１と通信を行うことが可能である。ＩＣカード１１４１は、ユーザＩＤなどの各種のデータが記憶しており、ＳＡＭ３０５$_1$においてユーザ認証を行う場合などに用いられる。

【０４１２】

ＡＶ機器３６０$_2$は、例えば、ストレージ機器であり、ＳＡＭ３０５$_1$と３０５$_2$との間で所定の処理を経て、ＩＥＥＥ１３９４シリアルバス１９１を介してネットワーク機器３６０$_1$から入力したセキュアコンテナを記録媒体１３０に記録する。

また、ＡＶ機器３６０$_3$も同様に、例えば、ストレージ機器であり、ＳＡＭ３０５$_2$と３０５$_3$との間で所定の処理を経て、ＩＥＥＥ１３９４シリアルバス１９１を介してＡＶ機器３６０$_2$から入力したセキュアコンテナを記録媒体１３０に記録する。

【０４１３】

なお、図１０１に示す例では、記録媒体１３０にメディアＳＡＭ１３３が搭載されている場合を例示したが、例えば、記録媒体１３０のメディアＳＡＭ１３３が搭載されていない場合には、図１０１に点線で示したように、メディア・ドラブＳＡＭ２６０を用いて、ＳＡＭ３０５$_2$，３０５$_3$との間の認証が行われる。

【０４１４】

次に、図８２に示すＥＭＤシステム３００の全体動作について説明する。

図１０２および図１０３は、ＥＭＤシステム３００の全体動作のフローチャートである。

ここでは、サービスプロバイダ３１０からユーザホームネットワーク３０３にオンラインでセキュアコンテナ３０４を送信する場合を例示して説明する。

なお、以下に示す処理の前提として、ＥＭＤサービスセンタ３０２へのコンテンツプロバイダ３０１、サービスプロバイダ３１０およびＳＡＭ３０５$_1$～３０

5_4 の登録は既に終了しているものとする。

【０４１５】

ステップＳ２１：ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データ$K_{CP,P}$の公開鍵証明書CER_{CP}を、自らの署名データ$SIG_{1,ESC}$と共にコンテンツプロバイダ３０１に送信する。

また、ＥＭＤサービスセンタ３０２は、コンテンツプロバイダ３０１の公開鍵データ$K_{SP,P}$の公開鍵証明書CER_{SP}を、自らの署名データ$SIG_{61,ESC}$と共にサービスプロバイダ３１０に送信する。

また、ＥＭＤサービスセンタ３０２は、各々有効期限が１カ月の３カ月分のライセンス鍵データKD_1～KD_3をユーザホームネットワーク３０３のＳＡＭ305_1～305_4に送信する。

【０４１６】

ステップＳ２２：コンテンツプロバイダ３０１は、相互認証を行った後に、権利書データ１０６およびコンテンツ鍵データＫｃをＥＭＤサービスセンタ３０２に登録して権威化する。

また、ＥＭＤサービスセンタ３０２は、図３（Ｂ）に示す６カ月分のキーファイルＫＦを作成し、これをコンテンツプロバイダ３０１に送信する。

【０４１７】

ステップＳ２３：コンテンツプロバイダ３０１は、図３（Ａ），（Ｂ）に示すコンテンツファイルＣＦおよびその署名データ$SIG_{6,CP}$と、キーファイルＫＦおよびその署名データ$SIG_{7,CP}$とを作成し、これらと図３（Ｃ）に示す公開鍵証明書データCER_{cp}およびその署名データ$SIG_{1,ESC}$とを格納したセキュアコンテナ１０４を、オンラインおよび／またはオフラインで、サービスプロバイダ３１０に提供する。

【０４１８】

ステップＳ２４：サービスプロバイダ３１０は、図３（Ｃ）に示す署名データ$SIG_{1,ESC}$を検証した後に、公開鍵証明書データCER_{CP}に格納された公開鍵データ$K_{CP,P}$を用いて、図３（Ａ），（Ｂ）に示す署名データ$SIG_{6,CP}$および$SIG_{7,CP}$を検証して、セキュアコンテナ１０４が正当なコンテンツプロバイダ

３０１から送信されたものであるかを確認する。

【０４１９】

ステップＳ２５：サービスプロバイダ３１０は、プライスタグデータ３１２およびその署名データ$SIG_{64,SP}$を作成し、これらを格納したを格納した図８７に示すセキュアコンテナ３０４を作成する。

【０４２０】

ステップＳ２６：サービスプロバイダ３１０は、プライスタグデータ３１２をＥＭＤサービスセンタ３０２に登録して権威化する。

【０４２１】

ステップＳ２７：サービスプロバイダ３１０は、例えば、ユーザホームネットワーク３０３のＣＡモジュール３１１からの要求に応じて、ステップＳ２５で作成したセキュアコンテナ３０４を、オンラインあるいはオフラインで、図８９に示すネットワーク機器360_1の復号モジュール９０５に送信する。

【０４２２】

ステップＳ２８：ＣＡモジュール３１１は、ＳＰ用購入履歴データ３０９を作成し、これを所定のタイミングで、サービスプロバイダ３１０に送信する。

【０４２３】

ステップＳ２９：$SAM305_1$～305_4のいずれかにおいて、図８４（Ｄ）に示す署名データ$SIG_{61,ESC}$を検証した後に、公開鍵証明書データCER_{SP}に格納された公開鍵データ$K_{SP,P}$を用いて、図８４（Ａ），（Ｂ），（Ｃ）に示す署名データ$SIG_{62,SP}$，$SIG_{63,SP}$，$SIG_{64,SP}$を検証して、セキュアコンテナ３０４内の所定のデータが正当なサービスプロバイダ３１０において作成および送信されたか否かを確認する。

【０４２４】

ステップＳ３０：$SAM305_1$～305_4のいずれかにおいて、図８４（Ｄ）に示す署名データ$SIG_{1,ESC}$を検証した後に、公開鍵証明書データCER_{CP}に格納された公開鍵データ$K_{CP,P}$を用いて、図８４（Ａ），（Ｂ），（Ｃ）に示す署名データ$SIG_{6,SP}$，$SIG_{7,SP}$を検証して、セキュアコンテナ３０４内のコンテンツファイルＣＦが正当なコンテンツプロバイダ３０１において作成され

たか否かと、キーファイルＫＦが正当なコンテンツプロバイダ３０１から送信されたか否かを確認する。

また、ＳＡＭ３０５$_1$～３０５$_4$のいずれかにおいて、公開鍵データ$K_{ESC,P}$を用いて、図８４（Ｂ）に示すキーファイルＫＦ内の署名データ$SIG_{K1,ESC}$の正当性を検証することで、キーファイルＫＦが正当なＥＭＤサービスセンタ３０２によって作成されたか否かを確認する。

【０４２５】

ステップＳ３１：ユーザが図８８に示す操作部１６５を操作してコンテンツの購入・利用形態を決定する。

【０４２６】

ステップＳ３２：ステップＳ３１においてホストＣＰＵ８１０からＳＡＭ３０５$_1$～３０５$_4$に出された内部割り込みＳ８１０に基づいて、ＳＡＭ３０５$_1$～３０５$_4$において、セキュアコンテナ３０４の利用履歴(Usage Log) データ３０８が生成される。

ＳＡＭ３０５$_1$～３０５$_4$からＥＭＤサービスセンタ３０２に、利用履歴データ３０８およびその署名データ$SIG_{205,SAM1}$が送信される。

また、購入形態が決定される度にリアルタイムに、ＳＡＭ３０５$_1$～３０５$_4$からＥＭＤサービスセンタ３０２に利用制御状態データ１６６が送信される。

【０４２７】

ステップＳ３３：ＥＭＤサービスセンタ３０２は、利用履歴データ３０８に基づいて、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の各々について、課金内容を決定（計算）し、その結果に基づいて、決済請求権データ１５２ｃ，１５２ｓを作成する。

【０４２８】

ステップＳ３４：ＥＭＤサービスセンタ３０２は、ペイメントゲートウェイ９０を介して決済機関９１に、決済請求権データ１５２ｃ，１５２ｓを自らの署名データと共に送信し、これにより、ユーザホームネットワーク３０３のユーザが決済機関９１に支払った金銭が、コンテンツプロバイダ３０１およびサービスプロバイダ３１０の所有者に分配される。

【０４２９】

以上説明したように、ＥＭＤシステム３００では、図３に示すフォーマットのセキュアコンテナ１０４をコンテンツプロバイダ３０１からサービスプロバイダ３１０に配給し、セキュアコンテナ１０４内のコンテンツファイルＣＦおよびキーファイルＫＦをそのまま格納したセキュアコンテナ３０４をサービスプロバイダ３１０からユーザホームネットワーク３０３に配給し、キーファイルＫＦについての処理をＳＡＭ305_1～305_4内で行う。

また、キーファイルＫＦに格納されたコンテンツ鍵データＫｃおよび権利書データ１０６は、配信鍵データKD_1～KD_3を用いて暗号化されており、配信鍵データKD_1～KD_3を保持しているＳＡＭ305_1～305_4内でのみ復号される。そして、ＳＡＭ305_1～305_4では、耐タンパ性を有するモジュールであり、権利書データ１０６に記述されたコンテンツデータＣの取り扱い内容に基づいて、コンテンツデータＣの購入形態および利用形態が決定される。

【０４３０】

従って、ＥＭＤシステム３００によれば、ユーザホームネットワーク３０３におけるコンテンツデータＣの購入および利用を、サービスプロバイダ３１０における処理とは無関係に、コンテンツプロバイダ３０１の関係者が作成した権利書データ１０６の内容に基づいて確実に行わせることができる。すなわち、ＥＭＤシステム３００によれば、権利書データ１０６をサービスプロバイダ３１０が管理できないようできる。

そのため、ＥＭＤシステム３００によれば、異系列の複数のサービスプロバイダ３１０を介してユーザホームネットワーク３０３にコンテンツデータＣが配給された場合でも、ユーザホームネットワーク３０３のＳＡＭにおける当該コンテンツデータＣについての権利処理を、コンテンツプロバイダ３０１が作成した共通の権利書データ１０６に基づいて行わせることができる。

【０４３１】

また、ＥＭＤシステム３００では、セキュアコンテナ１０４，３０４内の各ファイルおよびデータについて、それらの作成者および送信者の正当性を示す署名データを格納していることから、サービスプロバイダ３１０およびＳＡＭ３０５

$_1$～３０５$_4$において、それらの作成者および送信者の正当性、並びにそれらが改竄されていないか否かなどを確認できる。その結果、コンテンツデータＣの不正利用を効果的に回避できる。

【０４３２】

また、ＥＭＤシステム３００では、サービスプロバイダ３１０からユーザホームネットワーク３０３へのコンテンツデータＣの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ３０４を用いて行うことで、双方の場合において、ＳＡＭ３０５$_1$～３０５$_4$におけるコンテンツデータＣの権利処理を共通化できる。

【０４３３】

また、ＥＭＤシステム３００では、ユーザホームネットワーク３０３内のネットワーク機器３６０$_1$およびＡＶ機器３６０$_2$～３６０$_4$においてコンテンツデータＣを購入、利用、記録および転送する際に、常に権利書データ１０６に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

例えば、図１０４に示すように、コンテンツプロバイダ３０１が提供したコンテンツデータＣを、サービスプロバイダ３１０からユーザホームネットワーク３０３に、パッケージ流通、デジタル放送、インターネット、専用線、デジタルラジオおよびモバイル通信などの何れの手法（経路）で配信（配給）した場合でも、ユーザホームネットワーク３０３，３０３ａのＳＡＭにおいて、コンテンツプロバイダ３０１が作成した権利書データ１０６に基づいて、共通の権利処理ルールが採用される。

【０４３４】

また、ＥＭＤシステム３００によれば、ＥＭＤサービスセンタ３０２が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ３０１およびＥＭＤサービスセンタ３０２の所有者に、予め決められた比率に従って確実に分配される。

また、ＥＭＤシステム３００によれば、同じコンテンツプロバイダ３０１が供給した同じコンテンツファイルＣＦについての権利書データ１０６は、サービス

プロバイダ３１０のサービス形態とは無関係に、そのままＳＡＭ３０$5_1$～３０$5_4$に供給される。従って、ＳＡＭ３０$5_1$～３０$5_4$において、権利書データ１０６に基づいて、コンテンツプロバイダ３０１の意向通りに、コンテンツファイルＣＦの利用を行わせることができる。

すなわち、ＥＭＤシステム３００によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織７２５に頼ることなく、技術的な手段によって、コンテンツプロバイダ３０１の所有者の権利および利益を確実に守ることができる。

【０４３５】

以下、上述した第２実施形態のＥＭＤシステム３００で採用するセキュアコンテナなどの配送プロトコルについて説明する。

図１０５に示すように、コンテンツプロバイダ３０１において作成されたセキュアコンテナ１０４は、インターネット（ＴＣＰ／ＩＰ）あるいは専用線（ＡＴＭ　Ｃｅｌｌ）などのコンテンツプロバイダ用配送プロトコルを用いてサービスプロバイダ３１０に提供される。

また、サービスプロバイダ３１０は、セキュアコンテナ１０４を用いて作成したセキュアコンテナ３０４を、デジタル放送（ＭＰＥＧ－ＴＳ上のＸＭＬ／ＳＭＩＬ）、インターネット（ＴＣＰ／ＩＰ上のＸＭＬ／ＳＭＩＬ）あるいはパッケージ流通（記録媒体）などのサービスプロバイダ用配送プロトコルを用いてユーザホームネットワーク３０３に配給する。

また、ユーザホームネットワーク３０３，３０３ａ内、あるいはユーザホームネットワーク３０３と３０３ａとの間において、ＳＭＡ相互間で、セキュアコンテナが、家庭内ＥＣ(Electric Commerce)／配信サービス（１３９４シリアルバス・インターフェイス上のＸＭＬ／ＳＭＩＬ）や記録媒体などを用いて転送される。

【０４３６】

本発明は上述した実施形態には限定されない。

例えば、上述した実施形態では、ＥＭＤサービスセンタ１０２，３０２において、キーファイルＫＦを作成する場合を例示したが、コンテンツプロバイダ１０

１，３０１においてキーファイルＫＦを作成してもよい。

【０４３７】

【発明の効果】

以上説明したように、本発明のデータ処理装置によれば、コンテンツデータの取り扱いを示す権利書データに基づいたコンテンツデータの権利処理をセキュアな環境で行うことができる。

その結果、権利書データをコンテンツデータの提供に係わる者が作成すれば、コンテンツデータに係わる利益を適切に保護することが可能になると共に、当該関係者による監査の負担を軽減できる。

【図面の簡単な説明】

【図１】

図１は、本発明の第１実施形態のＥＭＤシステムの全体構成図である。

【図２】

図２は、本発明のセキュアコンテナの概念を説明するための図である。

【図３】

図３は、図１に示すコンテンツプロバイダからＳＡＭに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図４】

図４は、図３に示すコンテンツファイルに含まれるデータを詳細に説明するための図である。

【図５】

図５は、図３に示すキーファイルに含まれるデータを詳細に説明するための図である。

【図６】

図６は、図１に示すコンテンツプロバイダとＥＭＤサービスセンタとの間で行われる登録およびキーファイルの転送を説明するための図である。

【図７】

図７は、コンテンツファイルに格納されるヘッダデータを説明するための図である。

【図８】

図８は、コンテンツＩＤを説明するための図である。

【図９】

図９は、セキュアコンテナのディレクトリ構造を説明するための図である。

【図１０】

図１０は、セキュアコンテナのハイパーリンク構造を説明するための図である。

【図１１】

図１１は、本実施形態で用いられるＲＯＭ型の記録媒体の第１の例を説明するための図である。

【図１２】

図１２は、本実施形態で用いられるＲＯＭ型の記録媒体の第２の例を説明するための図である。

【図１３】

図１３は、本実施形態で用いられるＲＯＭ型の記録媒体の第３の例を説明するための図である。

【図１４】

図１４は、本実施形態で用いられるＲＡＭ型の記録媒体の第１の例を説明するための図である。

【図１５】

図１５は、本実施形態で用いられるＲＡＭ型の記録媒体の第２の例を説明するための図である。

【図１６】

図１６は、本実施形態で用いられるＲＡＭ型の記録媒体の第３の例を説明するための図である。

【図１７】

図１７は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図１８】

図１８は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図１９】

図１９は、コンテンツプロバイダにおけるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図２０】

図２０は、図１に示すＥＭＤサービスセンタの機能を示す図である。

【図２１】

図２１は、図１に示す利用履歴データを説明するための図である。

【図２２】

図２２は、図１に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図２３】

図２３は、図２２に示すホストＣＰＵとＳＡＭとの関係を説明するための図である。

【図２４】

図２４は、ＳＡＭを実現するソフトウェア構成を説明するための図である。

【図２５】

図２５は、ホストＣＰＵに出される外部割り込みを説明するための図である。

【図２６】

図２６は、ホストＣＰＵが出す内部割り込みを説明するための図である。

【図２７】

図２７は、ホストＣＰＵが出すファンクションコールを説明するための図である。

【図２８】

図２８は、ＳＡＭのＣＰＯＵの処理状態を説明するための図である。

【図２９】

図２９は、ホストＣＰＵおよびＳＡＭのメモリ空間を説明するための図である

。

【図３０】

図３０は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでのデータの流れを示す図である。

【図３１】

図３１は、図２２に示す外部メモリに記憶されるデータを説明するための図である。

【図３２】

図３２は、作業用メモリに記憶されるデータを説明するための図である。

【図３３】

図３３は、図１に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図３４】

図３４は、図３０に示す記憶部に記憶されるデータを説明するための図である。

。

【図３５】

図３５は、ＥＭＤサービスセンタからライセンス鍵データを受信する際のＳＡＭの処理を示すフローチャートである。

【図３６】

図３６は、セキュアコンテナを入力する際のＳＡＭの処理を示すフローチャートである。

【図３７】

図３７は、図１に示すユーザホームネットワーク内のＳＡＭの機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図３８】

図３８は、コンテンツデータの購入形態を決定する際のＳＡＭの処理を示すフローチャートである。

【図３９】

図３９は、購入形態が決定されたセキュアコンテナを説明するための図である。

【図４０】

図４０は、コンテンツデータを再生する際のＳＡＭの処理を示すフローチャートである。

【図４１】

図４１は、図２２に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送し、ＡＶ機器において再購入を行う場合を説明するための図である。

【図４２】

図４２は、図４１に示す場合における転送元のＳＡＭ内でのデータの流れを示す図である。

【図４３】

図４３は、図４２に示す場合の処理を示すフローチャートである。

【図４４】

図４４は、図４１において転送されるセキュアコンテナのフォーマットを説明するための図である。

【図４５】

図４５は、図４１に示す場合において、転送先のＳＡＭにおいて、入力したコンテンツファイルなどを、ＲＡＭ型あるいはＲＯＭ型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図４６】

図４６は、図４１に示す場合における転送先のＳＡＭの処理を示すフローチャートである。

【図４７】

図４７は、図４１に示す場合における転送先のＳＡＭの処理を示すフローチャートである。

【図４８】

図４８は、図１に示すユーザホームネットワーク内のＳＡＭにおける各種の購入形態を説明するための図である。

【図４９】

図４９は、コンテンツの購入形態が未決定の図１１に示すＲＯＭ型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、ＡＶ機器において購入形態を決定する場合を説明するための図である。

【図５０】

図５０は、図４９に示す場合におけるＡＶ機器のＳＡＭ内でのデータの流れを示す図である。

【図５１】

図５１は、図４９に示す場合におけるＳＡＭの処理のフローチャートである。

【図５２】

図５２は、ユーザホームネットワーク内のＡＶ機器において購入形態が未決定のＲＯＭ型の記録媒体からセキュアコンテナを読み出して、これを他のＡＶ機器に転送してＲＡＭ型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図５３】

図５３は、図５２に示す場合における転送元のＳＡＭ内でのデータの流れを示す図である。

【図５４】

図５４は、図５２において、転送元のＳＡＭから転送先のＳＡＭに転送されるセキュアコンテナのフォーマットを説明するための図である。

【図５５】

図５５は、図５２の場合における、転送元および転送先のＳＡＭの処理のフローチャートを示す図である。

【図５６】

図５６は、図５２の場合における、転送元および転送先のＳＡＭの処理のフローチャートを示す図である。

【図５７】

図５７は、図５２に示す場合における転送先のＳＡＭ内でのデータの流れを示す図である。

【図５８】

図５８は、ユーザホームネットワーク内でのバスへの機器の接続形態の一例を説明するための図である。

【図５９】

図５９は、ＳＡＭが作成するＳＡＭ登録リストのデータフォーマットを説明するための図である。

【図６０】

図６０は、ＥＭＤサービスセンタが作成する公開鍵証明書破棄リストのフォーマットを説明するための図である。

【図６１】

図６１は、ＥＭＤサービスセンタが作成するＳＡＭ登録リストのデータフォーマットを説明するための図である。

【図６２】

図６２は、ＳＡＭが持つセキュリティ機能を説明するための図である。

【図６３】

図６２は、図１に示すユーザホームネットワーク内の例えばネットワーク機器内での各種のＳＡＭに搭載形態の一例を説明するための図である。

【図６４】

図６４は、図６３に示すダウンロードメモリ周辺の詳細な回路構成を説明するための図である。

【図６５】

図６５は、図６３におけるホストＣＰＵとＳＡＭとの関係を説明するための図である。

【図６６】

図６６は、図６３におけるホストＣＰＵ、ＳＡＭ、ＡＶ圧縮・伸長用ＳＡＭおよび記録媒体の関係を説明するための図である。

【図６７】

図６７は、図６３におけるホストＣＰＵＯ、メディア・ドラブＳＡＭおよびＡＶ圧縮・伸長用ＳＡＭの関係を説明するための図である。

【図６８】

図６８は、権利処理用のＳＡＭの回路モジュールの第１形態を説明するための図である。

【図６９】

図６９は、図６８に示す回路モジュールを用いた場合のＳＡＭ内のハードウェア構成の一例を説明するための図である。

【図７０】

図７０は、権利処理用のＳＡＭのアドレス空間を説明するための図である。

【図７１】

図７１は、ホストＣＰＵのアドレス空間を説明するための図である。

【図７２】

図７２は、権利処理用のＳＡＭの回路モジュールの第２形態を説明するための図である。

【図７３】

図７３は、メデャアＳＡＭの回路モジュールを説明するための図である。

【図７４】

図７４は、ＲＯＭ型の記録媒体のメディアＳＡＭの出荷時における記憶データを説明するための図である。

【図７５】

図７５は、ＲＯＭ型の記録媒体のメディアＳＡＭの登録後における記憶データを説明するための図である。

【図７６】

図７６は、ＲＡＭ型の記録媒体のメディアＳＡＭの出荷時における記憶データを説明するための図である。

【図７７】

図７７は、ＲＡＭ型の記録媒体のメディアＳＡＭの登録後における記憶データ

を説明するための図である。

【図７８】

図７８は、ＡＶ圧縮・伸長用ＳＡＭの回路モジュールの第１形態を説明するための図である。

【図７９】

図７９は、メディア・ドライブＳＡＭの回路モジュールを説明するための図である。

【図８０】

図８０は、図１に示すＥＭＤシステムの全体動作のフローチャートである。

【図８１】

図８１は、第１実施形態のＥＭＤシステムにおいて用いられるセキュアコンテナの配送プロトコルの一例を説明するための図である。

【図８２】

図８２は、本発明の第２実施形態のＥＭＤシステムの全体構成図である。

【図８３】

図８３は、サービスプロバイダにおいて行われるセキュアコンテナの作成処理の手順を示すフローチャートである。

【図８４】

図８４は、図８２に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図８５】

図８５は、図８４に示すセキュアコンテナに格納されたコンテンツファイルの送信形態を説明するための図である。

【図８６】

図８６は、図８７に示すセキュアコンテナに格納されたキーファイルの送信形態を説明するための図である。

【図８７】

図８７は、図８１に示すＥＭＤサービスセンタの機能を示す図である。

【図８８】

図８８は、図８２に示すネットワーク機器の構成図である。

【図８９】

図８９は、図８８に示すＣＡモジュールの機能ブロック図である。

【図９０】

図９０は、図８２に示すＳＡＭの機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図９１】

図９１は、図９０に示す作業用メモリに記憶されるデータを説明するための図である。

【図９２】

図９２は、図８２に示すＳＡＭの機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図９３】

図９３は、図８２に示すＳＡＭにおけるセキュアコンテナの入力処理の手順を示すフローチャートである。

【図９４】

図９４は、図８２に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合を説明するための図である。

【図９５】

図９５は、図８２に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、ＡＶ機器のＳＡＭに転送する場合の転送元のＳＡＭ内での処理の流れを説明するための図である。

【図９６】

図９６は、図９５に示す転送元のＳＡＭの処理を示すフローチャートである。

【図９７】

図９７は、図９４に示す場合に、転送元のＳＡＭから転送先のＳＡＭに転送されるセキュアコンテナのフォーマットを示す図である。

【図９８】

図９８は、図９４に示す場合の転送先のＳＡＭ内でのデータの流れを示す図である。

【図９９】

図９９は、図９４に示す場合の転送先のＳＡＭの処理のフローチャートである。

【図１００】

図１００は、図９４に示す場合の転送先のＳＡＭの処理のフローチャートである。

【図１０１】

図１０１は、図８２に示すユーザホームネットワーク内でのＳＡＭの接続形態の一例を説明するための図である。

【図１０２】

図１０２は、図８２に示すＥＭＤシステムの全体動作のフローチャートである。

【図１０３】

図１０３は、図８２に示すＥＭＤシステムの全体動作のフローチャートである。

【図１０４】

図１０４は、図８２に示すＥＭＤシステムのサービス形態の一例を示す図である。

【図１０５】

図１０５は、図８２に示すＥＭＤシステムにおいて採用されるセキュアコンテナの配送プロトコルを説明するための図である。

【図１０６】

図１０６は、従来のＥＭＤシステムの構成図である。

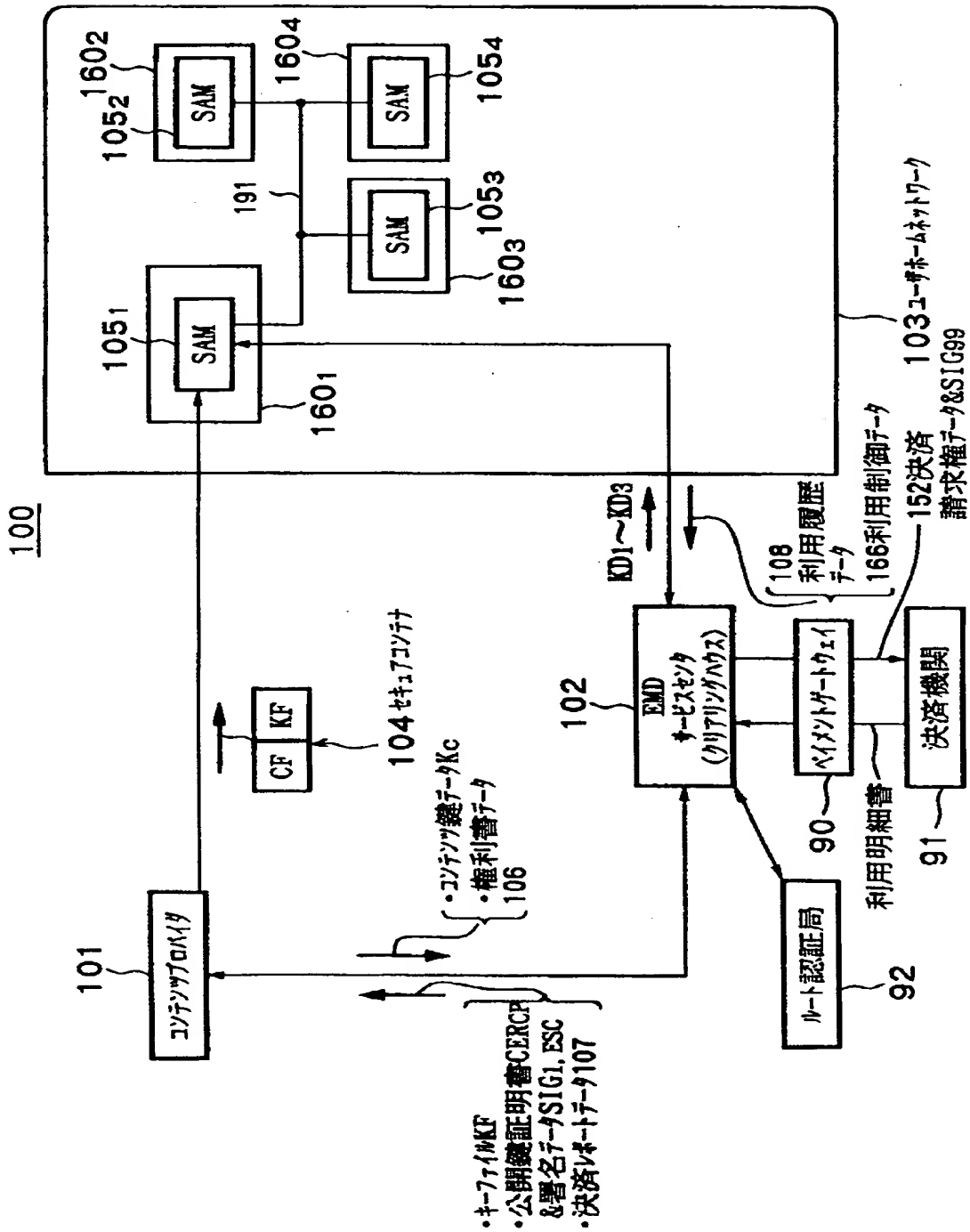
【符号の説明】

９０…ペイメントゲートウェイ、９１…決済機関、９２…ルート認証局、１００，３００…ＥＭＤシステム、１０１，３０１…コンテンツプロバイダ、１０２

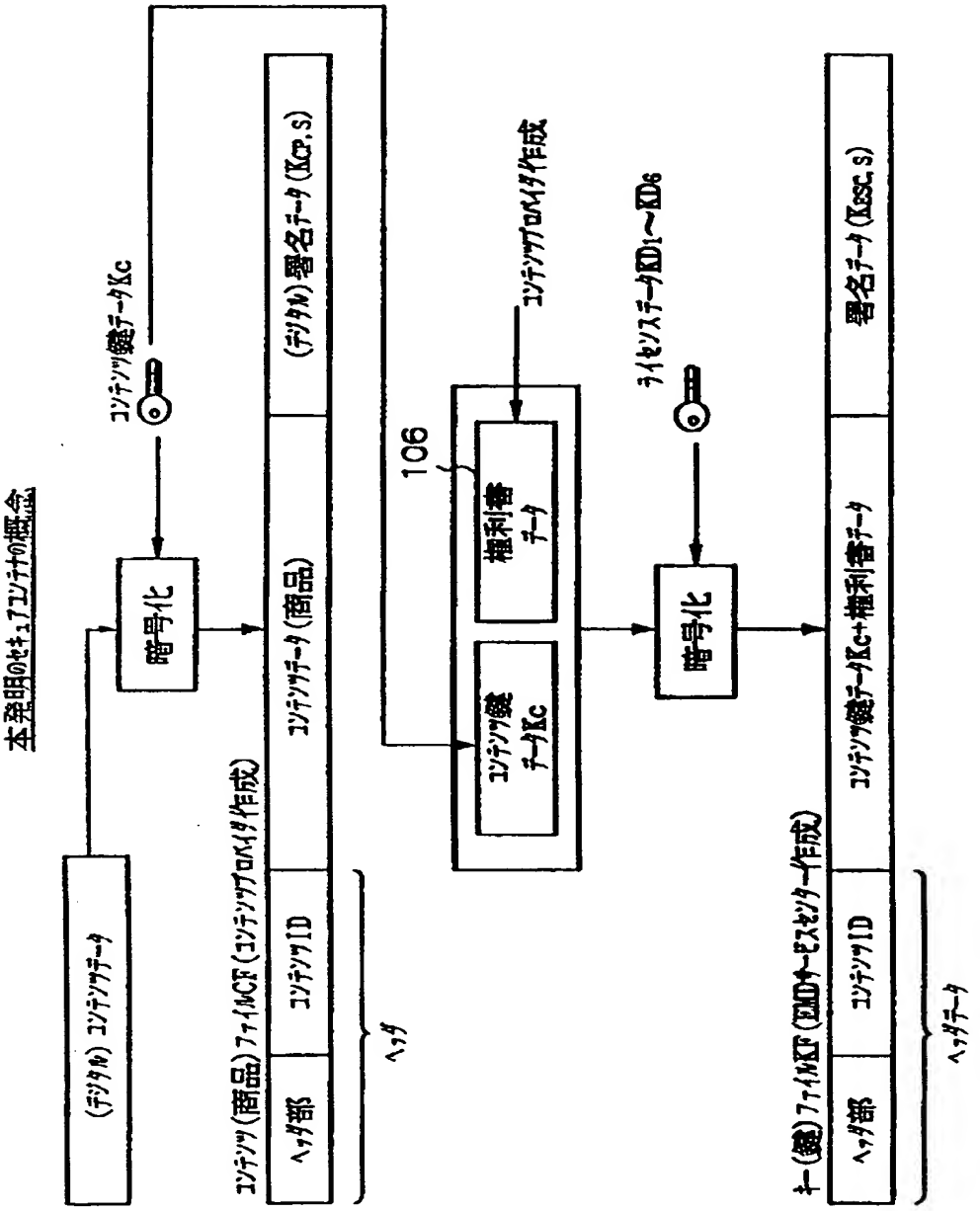
，３０２…ＥＭＤサービスセンタ、１０３，３０３…ユーザホームネットワーク、１０４，３０４…セキュアコンテナ、105_1～105_4，305_1～305_4…ＳＡＭ、１０６…権利書データ、１０７，３０７…決済レポートデータ、１０８，３０８…利用履歴データ、160_1…ネットワーク機器、160_2～160_4…ＡＶ機器、１５２，１５２ｃ，１５２ｓ…決済請求権データ、１９１…バス、３１０…サービスプロバイダ、３１１…ＣＡモジュール、３１２…プライスタグデータ、ＣＦ…コンテンツファイル、ＫＦ…キーファイル、Ｋｃ…コンテンツ鍵データ

【書類名】　図面

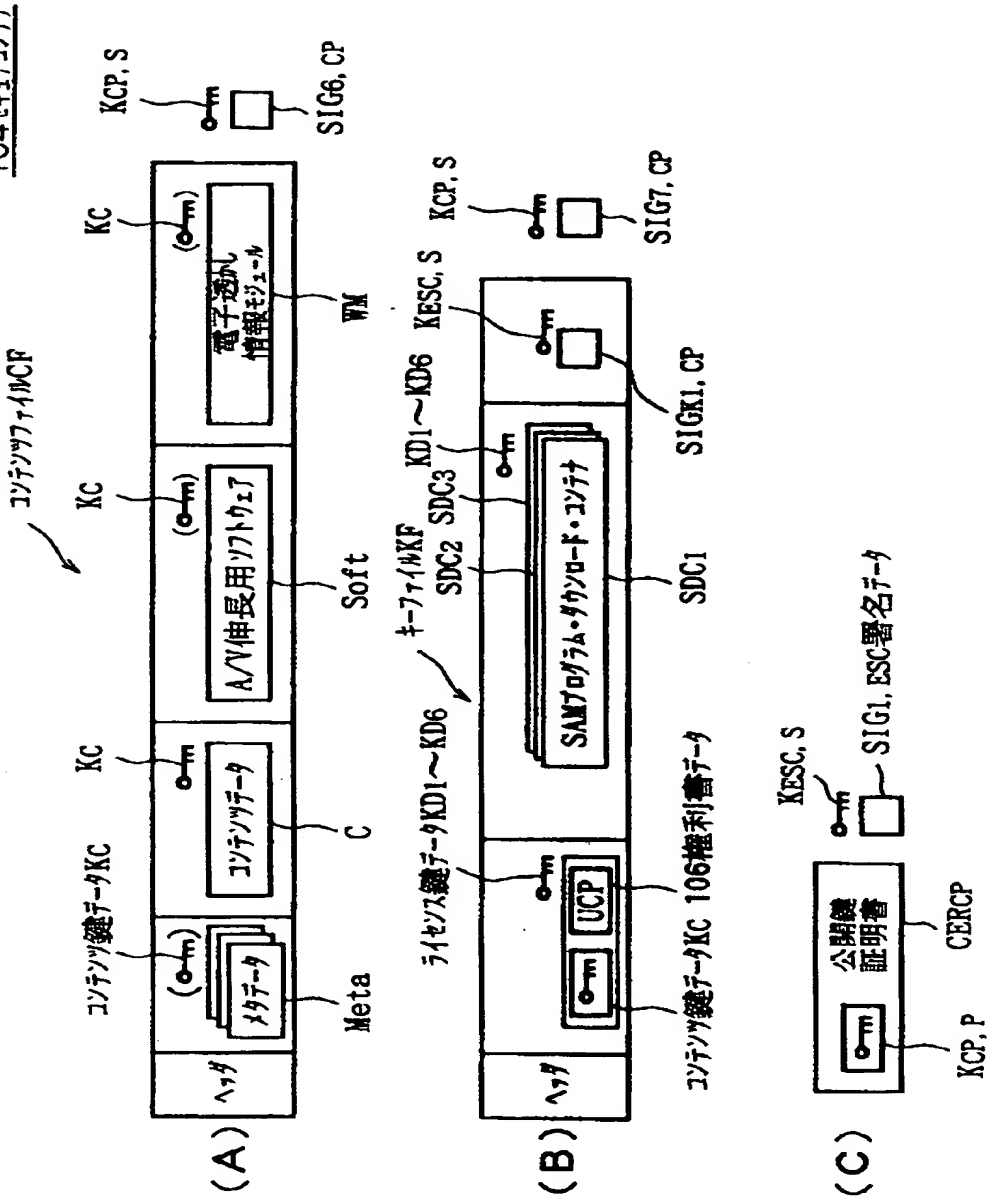
【図１】


100
SAM
1602
1052
1604
1054
191
1053
1603
1051
1601
103ユーザホームネットワーク
152決済
請求権データ&SIG99
KD1～KD3
108
利用履歴
データ
166利用制御データ
102
EMD
サービスセンタ
(クリアリングハウス)
ペイメントゲートウェイ
決済機関
90
91
利用明細書
ルート認証局
92
104セキュアコンテナ
CF
KF
・コンテンツ鍵データKc
・権利書データ
106
101
コンテンツプロバイダ
・キーファイルKF
・公開鍵証明書CERCP
&署名データSIG1, ESC
・決済レポートデータ107

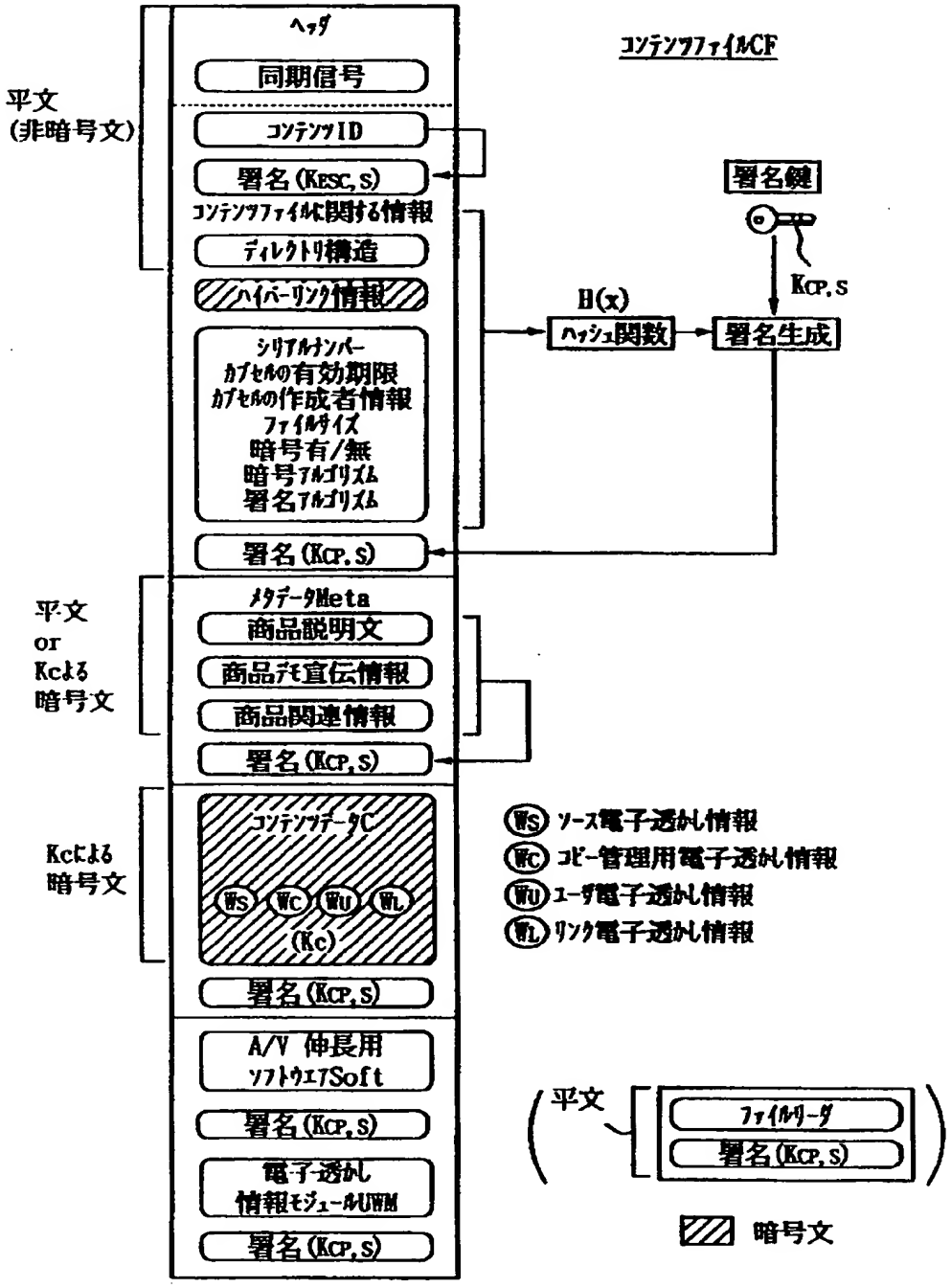
【図２】


本発明のセキュアコンテンツの概念
(デジタル) コンテンツデータ
暗号化
コンテンツ鍵データKc
コンテンツ(商品)ファイルCF(コンテンツプロバイダ作成)
ヘッダ部
コンテンツID
コンテンツデータ(商品)
(デジタル)署名データ(Kcp,s)
ヘッダ
106
コンテンツ鍵データKc
権利書データ
コンテンツプロバイダ作成
ライセンスデータKD1～KDn
暗号化
キー(鍵)ファイルKF(EMDサービスセンター作成)
ヘッダ部
コンテンツID
コンテンツ鍵データKc+権利書データ
署名データ(Kesc,s)
ヘッダデータ

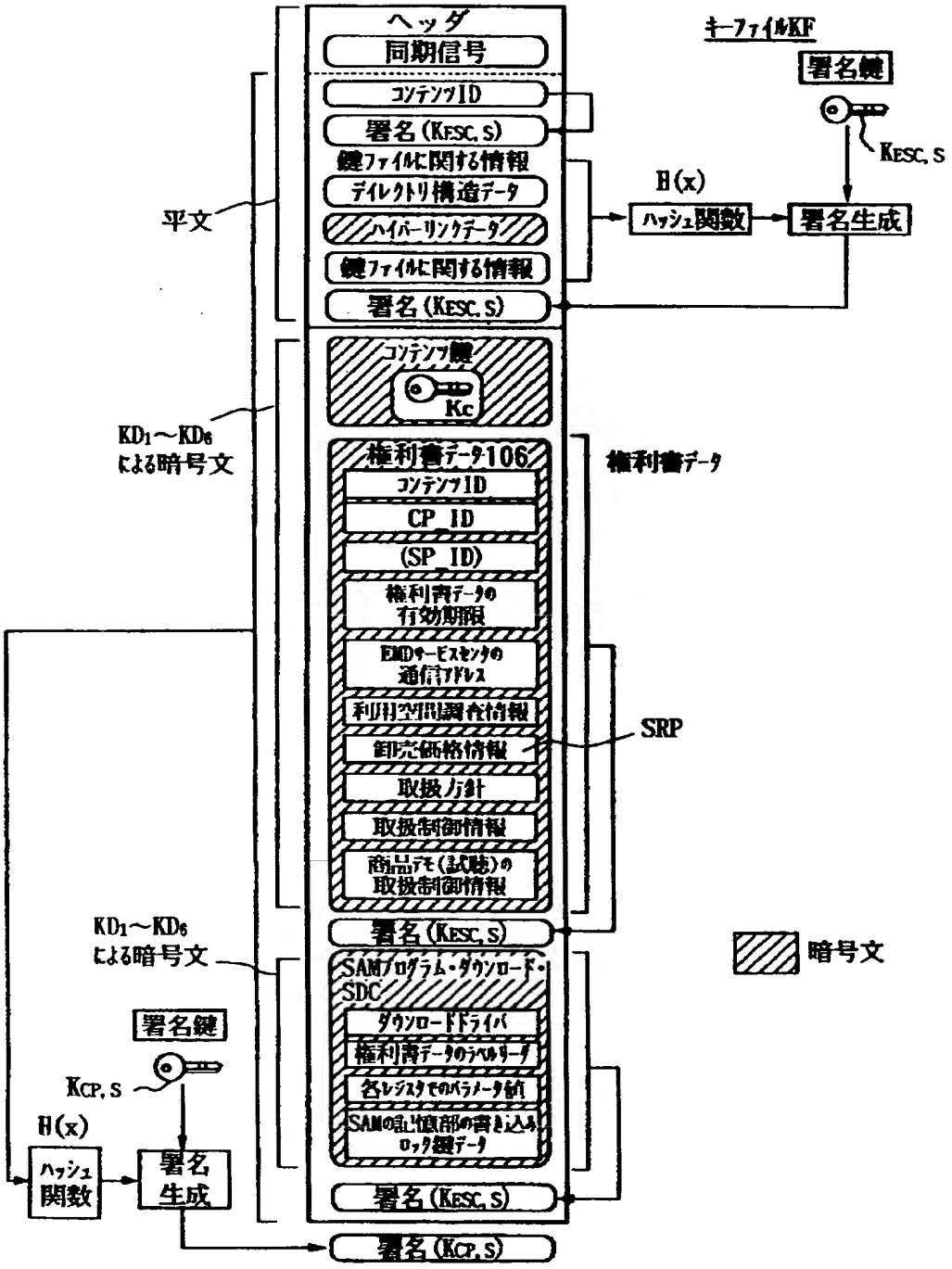
【図３】


104セキュアコンテナ
コンテンツファイルCF
Kc
Kc
Kc
KCP, S
SIG6, CP
電子透かし情報モジュール
WM
A/V伸長用ソフトウェア
Soft
コンテンツデータ
C
メタデータ
Meta
ヘッダ
(A)
コンテンツ鍵データKC
キーファイルKF
KD1～KD6
SDC2
SDC3
KD1～KD6
KESC, S
KCP, S
SIG7, CP
SIGK1, CP
SAMプログラム・ダウンロード・コンテナ
SDC1
UCP
ライセンス鍵データKD1～KD6
コンテンツ鍵データKc
106権利書データ
ヘッダ
(B)
KESC, S
SIG1, ESC署名データ
公開鍵証明書
CERCP
KCP, P
(C)

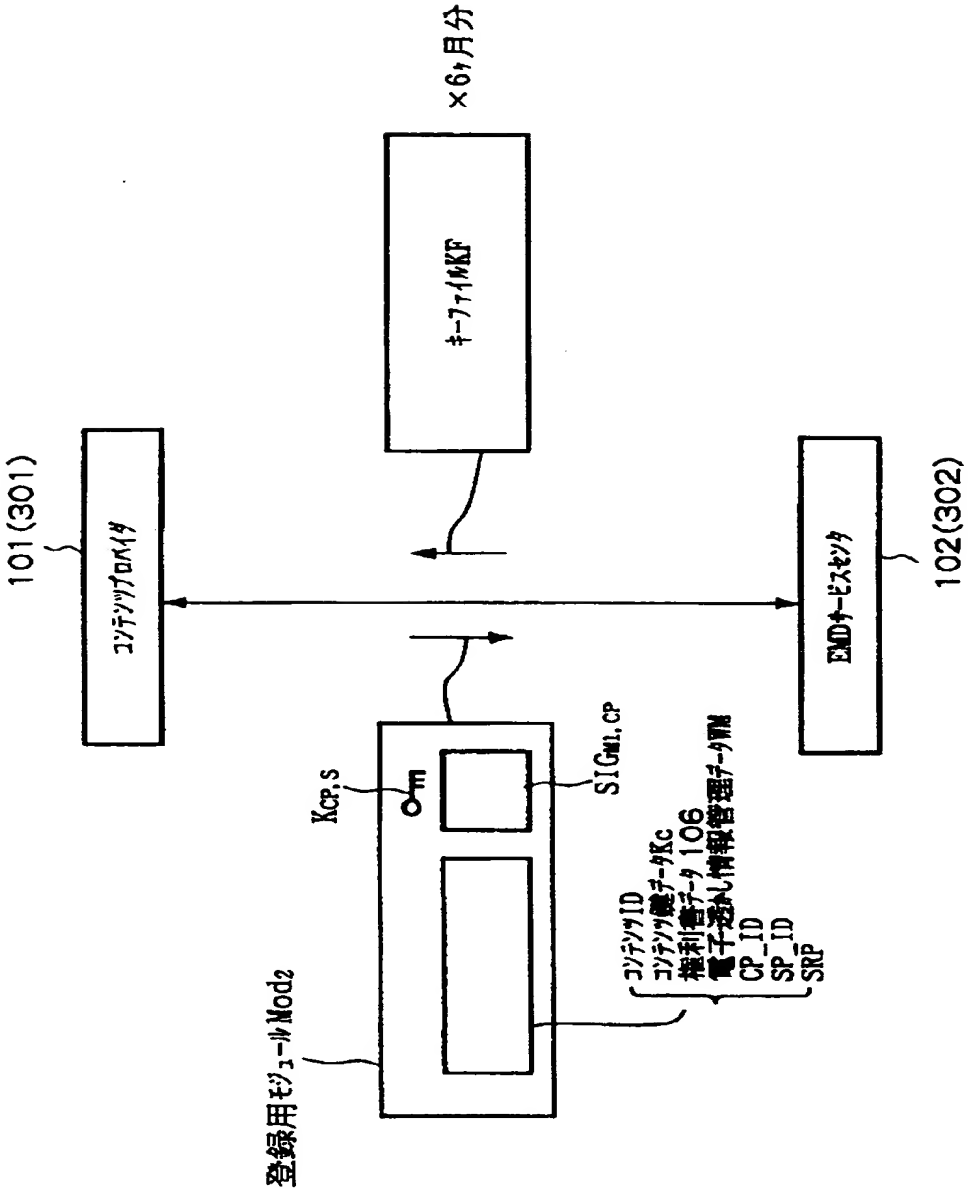
【図４】


ヘッダ
コンテンツファイルCF
同期信号
平文
(非暗号文)
コンテンツID
署名(KESC,S)
署名鍵
コンテンツファイルに関する情報
ディレクトリ構造
ハイパーリンク情報
KCP,S
H(x)
ハッシュ関数
署名生成
シリアルナンバー
カプセルの有効期限
カプセルの作成者情報
ファイルサイズ
暗号有/無
暗号アルゴリズム
署名アルゴリズム
署名(KCP,S)
メタデータMeta
平文
or
Kcよる
暗号文
商品説明文
商品デモ宣伝情報
商品関連情報
署名(KCP,S)
コンテンツデータC
Kcによる
暗号文
WS
WC
WU
WL
(Kc)
署名(KCP,S)
WS ソース電子透かし情報
WC コピー管理用電子透かし情報
WU ユーザ電子透かし情報
WL リンク電子透かし情報
A/V 伸長用
ソフトウエアSoft
署名(KCP,S)
電子透かし
情報モジュールUWM
署名(KCP,S)
平文
ファイルリーダ
署名(KCP,S)
暗号文

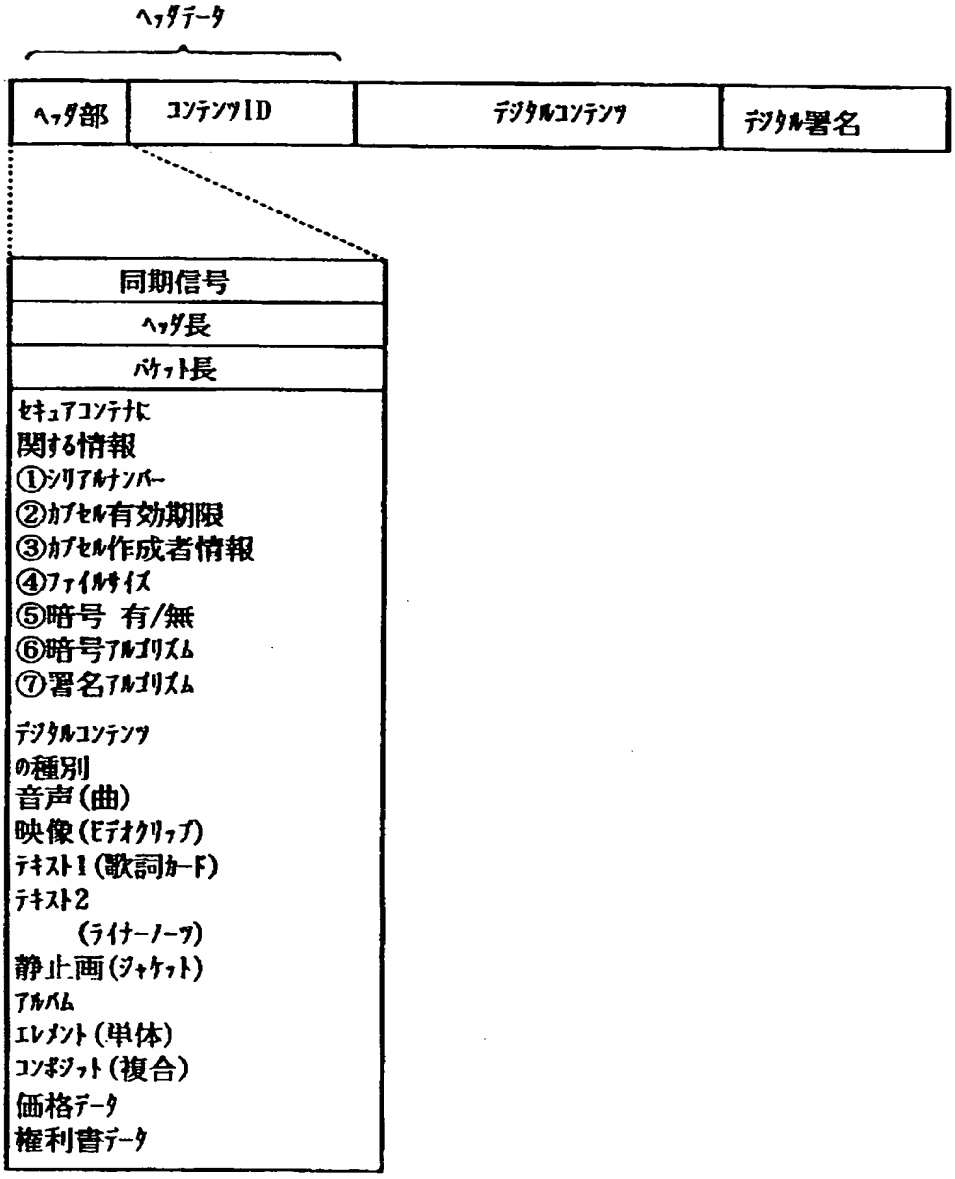
【図５】


ヘッダ
同期信号
コンテンツID
署名(KESC, S)
鍵ファイルに関する情報
ディレクトリ構造データ
ハイパーリンクデータ
鍵ファイルに関する情報
署名(KESC, S)
平文
キーファイルKF
署名鍵
KESC, S
H(x)
ハッシュ関数
署名生成
コンテンツ鍵
Kc
KD1～KD6
による暗号文
権利書データ106
コンテンツID
CP_ID
(SP_ID)
権利書データの
有効期限
EMDサービスセンタの
通信アドレス
利用空間調査情報
卸売価格情報
取扱方針
取扱制御情報
商品デモ(試聴)の
取扱制御情報
権利書データ
SRP
署名(KESC, S)
KD1～KD6
による暗号文
SAMプログラム・ダウンロード・
SDC
ダウンロードドライバ
権利書データのラベルリード
各レジスタでのパラメータ値
SAMの記憶部の書き込み
ロック鍵データ
暗号文
署名鍵
KCP, S
H(x)
ハッシュ関数
署名生成
署名(KESC, S)
署名(KCP, S)

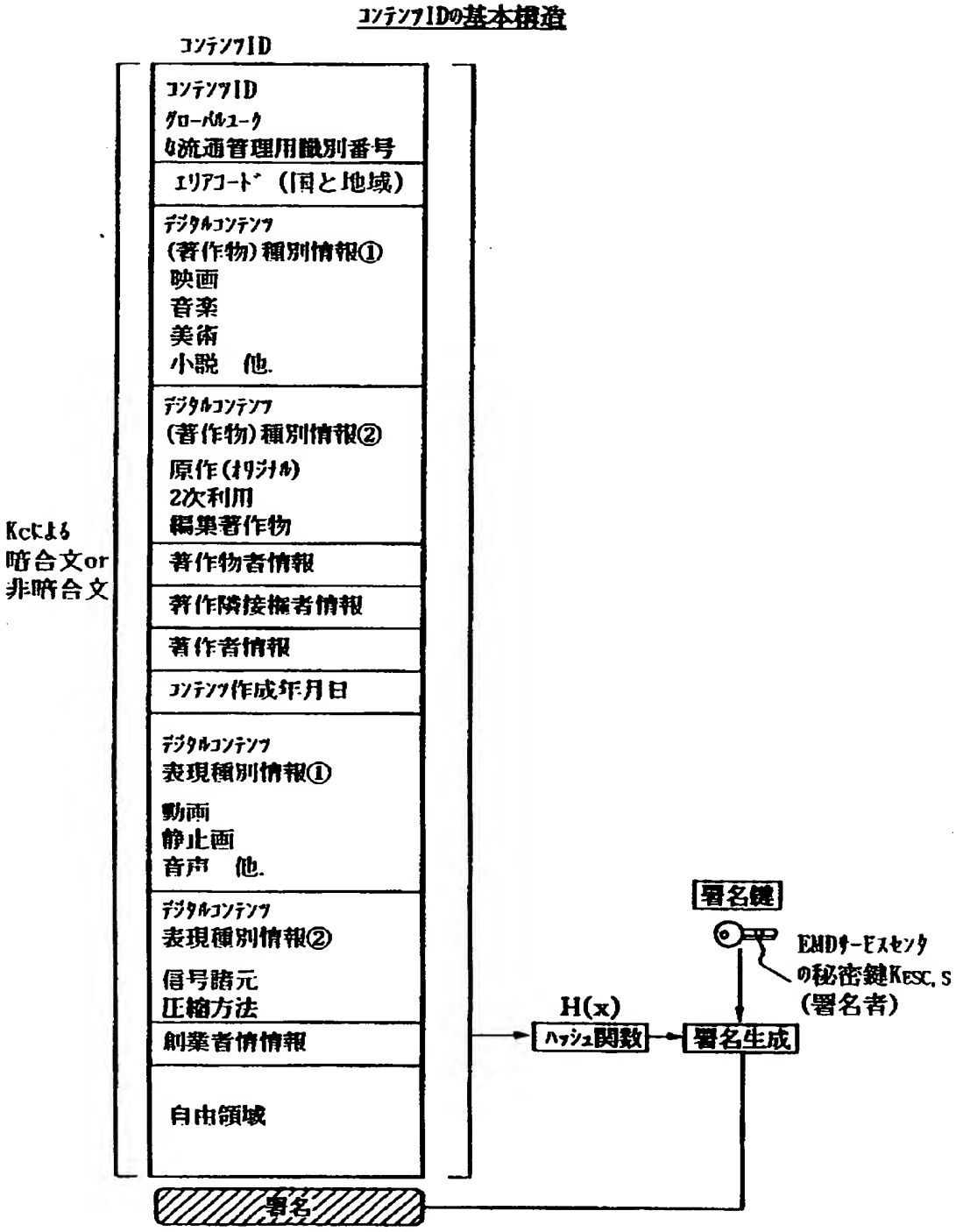
【図６】


×6ヶ月分
キーファイルKF
101(301)
コンテンツプロバイダ
102(302)
EMDサービスセンタ
登録用モジュールMod2
$K_{CP,S}$
$SIG_{M1,CP}$
コンテンツID
コンテンツ鍵データKc
権利情報データ106
電子透かし情報管理データTM
CP_ID
SP_ID
SRP

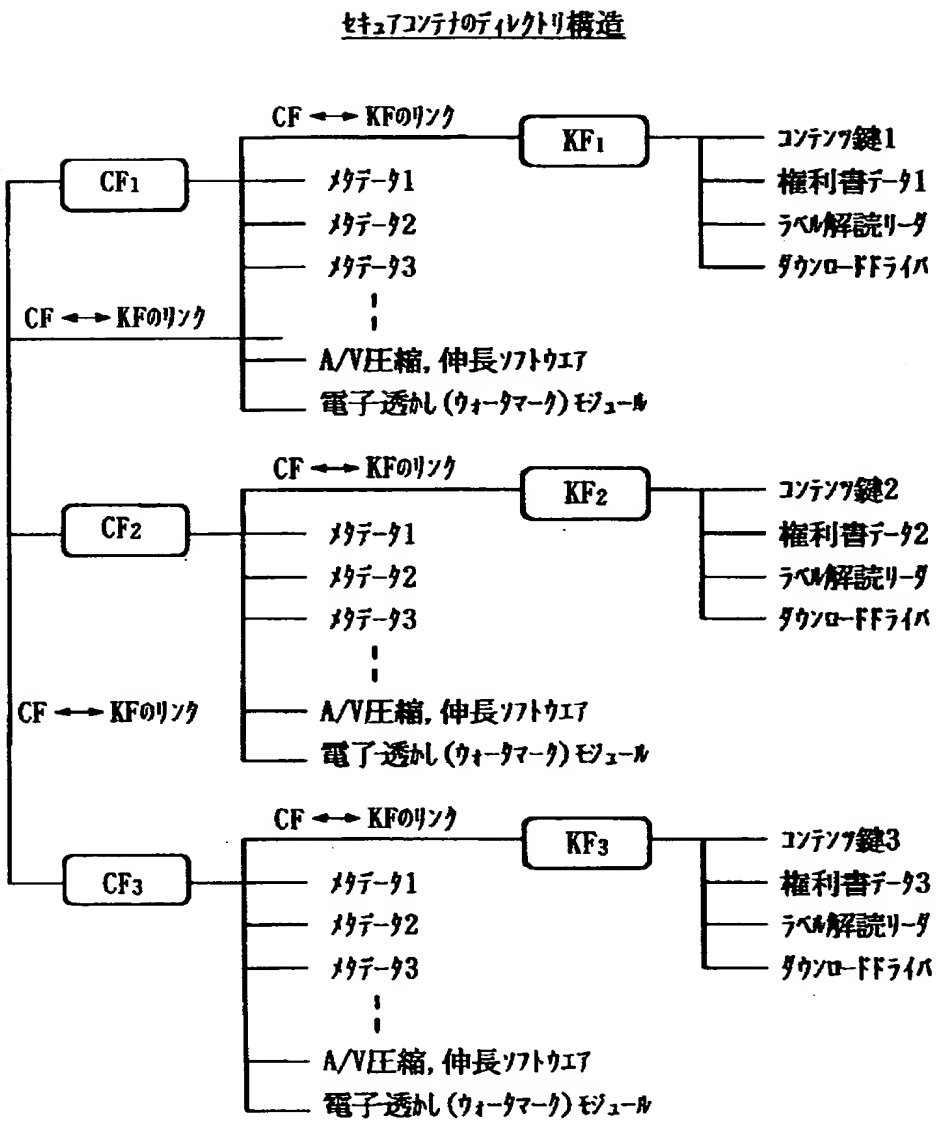
【図７】


ヘッダデータ
ヘッダ部
コンテンツID
デジタルコンテンツ
デジタル署名
同期信号
ヘッダ長
パケット長
セキュアコンテナに
関する情報
①シリアルナンバー
②カプセル有効期限
③カプセル作成者情報
④ファイルサイズ
⑤暗号 有/無
⑥暗号アルゴリズム
⑦署名アルゴリズム
デジタルコンテンツ
の種別
音声(曲)
映像(ビデオクリップ)
テキスト1(歌詞カード)
テキスト2
(ライナーノーツ)
静止画(ジャケット)
アルバム
エレメント(単体)
コンポジット(複合)
価格データ
権利書データ

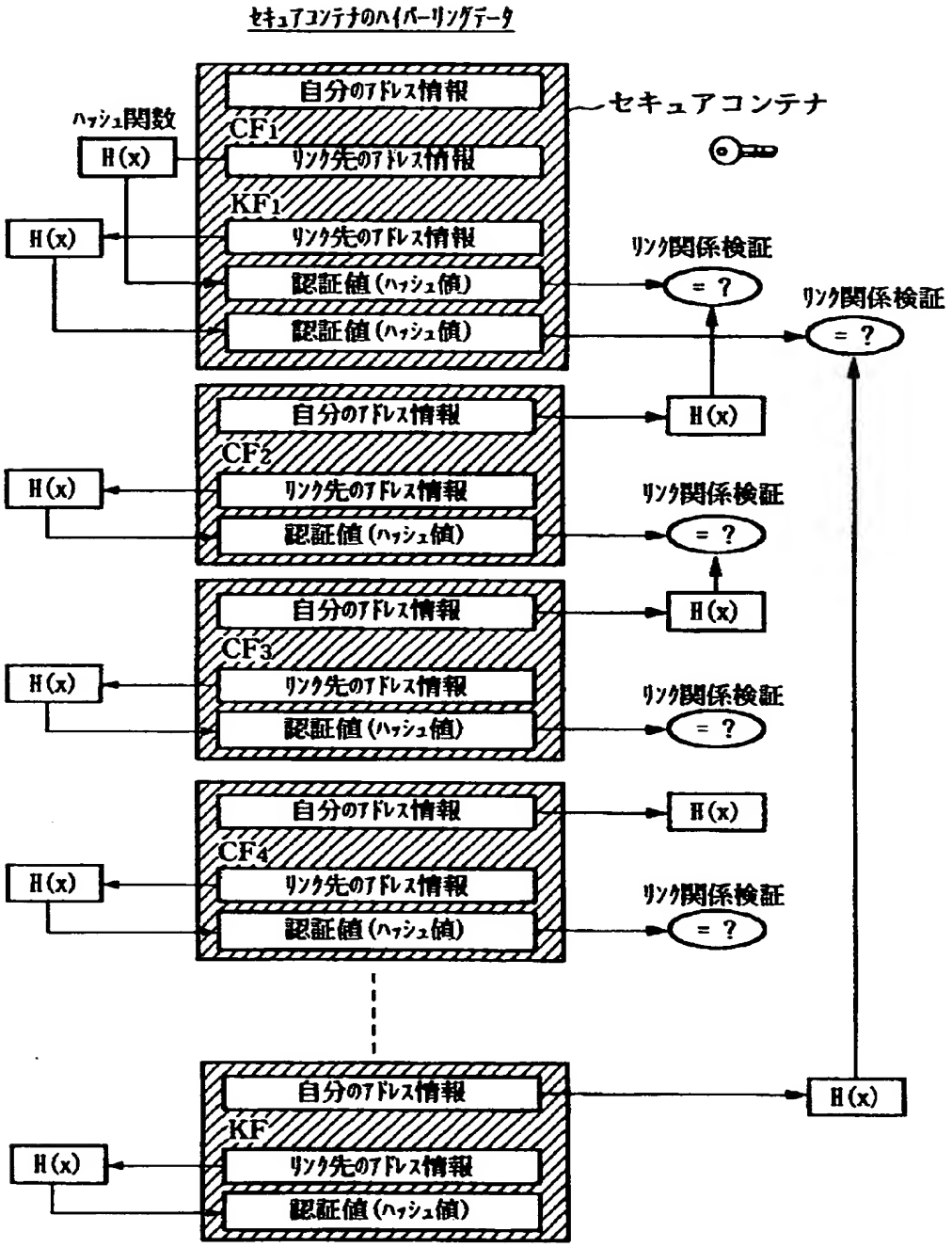
【図８】


コンテンツIDの基本構造
コンテンツID
コンテンツID
グローバルユーク
ゆ流通管理用識別番号
エリアコード（国と地域）
デジタルコンテンツ
(著作物)種別情報①
映画
音楽
美術
小説　他.
デジタルコンテンツ
(著作物)種別情報②
原作(オリジナル)
2次利用
編集著作物
著作物者情報
著作隣接権者情報
著作者情報
コンテンツ作成年月日
デジタルコンテンツ
表現種別情報①
動画
静止画
音声　他.
デジタルコンテンツ
表現種別情報②
信号諸元
圧縮方法
創業者情情報
自由領域
Kcによる
暗合文or
非暗合文
署名
署名鍵
EMDサービスセンタ
の秘密鍵Kesc, s
(署名者)
H(x)
ハッシュ関数
署名生成

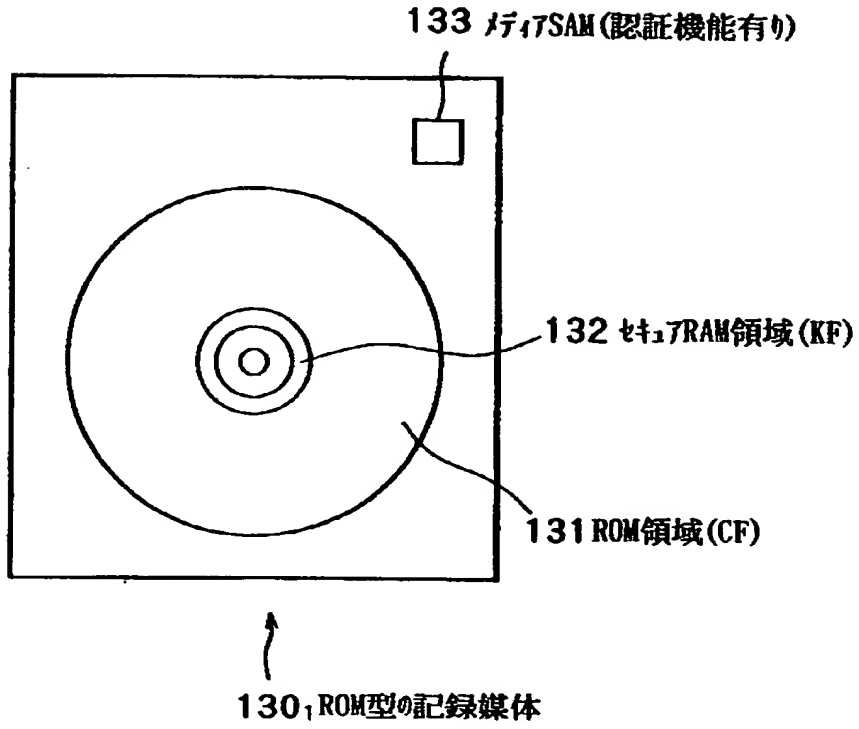
【図９】


セキュアコンテナのディレクトリ構造
CF ←→ KFのリンク
KF1
コンテンツ鍵1
権利書データ1
ラベル解読リーダ
ダウンロードドライバ
CF1
メタデータ1
メタデータ2
メタデータ3
CF ←→ KFのリンク
A/V圧縮，伸長ソフトウエア
電子透かし（ウォータマーク）モジュール
CF ←→ KFのリンク
KF2
コンテンツ鍵2
権利書データ2
ラベル解読リーダ
ダウンロードドライバ
CF2
メタデータ1
メタデータ2
メタデータ3
CF ←→ KFのリンク
A/V圧縮，伸長ソフトウエア
電子透かし（ウォータマーク）モジュール
CF ←→ KFのリンク
KF3
コンテンツ鍵3
権利書データ3
ラベル解読リーダ
ダウンロードドライバ
CF3
メタデータ1
メタデータ2
メタデータ3
A/V圧縮，伸長ソフトウエア
電子透かし（ウォータマーク）モジュール

【図１０】

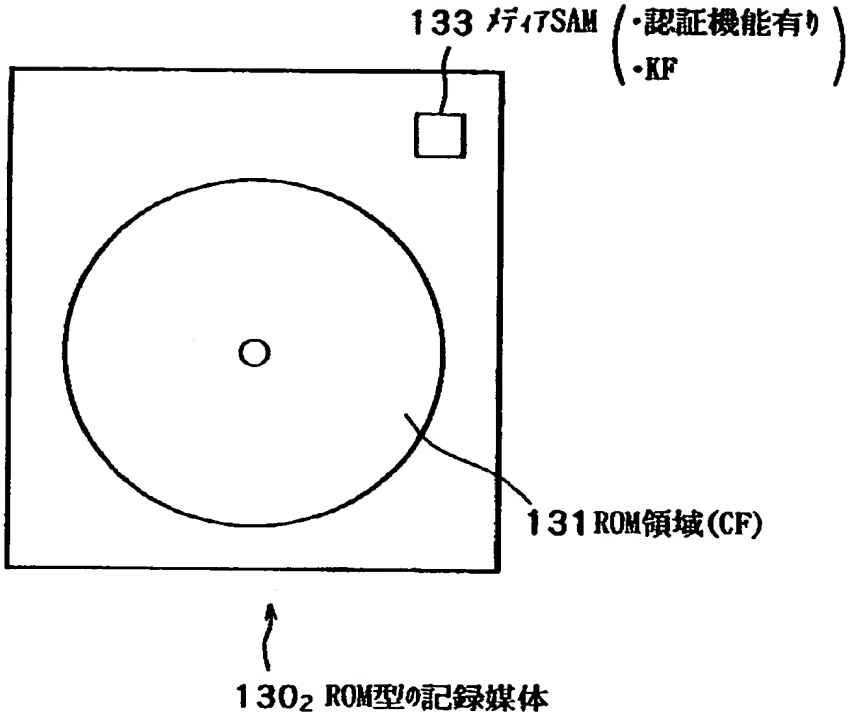

セキュアコンテナのハイパーリングデータ
ハッシュ関数
H(x)
CF1
自分のアドレス情報
リンク先のアドレス情報
KF1
リンク先のアドレス情報
認証値(ハッシュ値)
認証値(ハッシュ値)
セキュアコンテナ
リンク関係検証
= ?
リンク関係検証
= ?
CF2
自分のアドレス情報
リンク先のアドレス情報
認証値(ハッシュ値)
リンク関係検証
= ?
CF3
自分のアドレス情報
リンク先のアドレス情報
認証値(ハッシュ値)
リンク関係検証
= ?
CF4
自分のアドレス情報
リンク先のアドレス情報
認証値(ハッシュ値)
リンク関係検証
= ?
KF
自分のアドレス情報
リンク先のアドレス情報
認証値(ハッシュ値)
H(x)

【図１１】

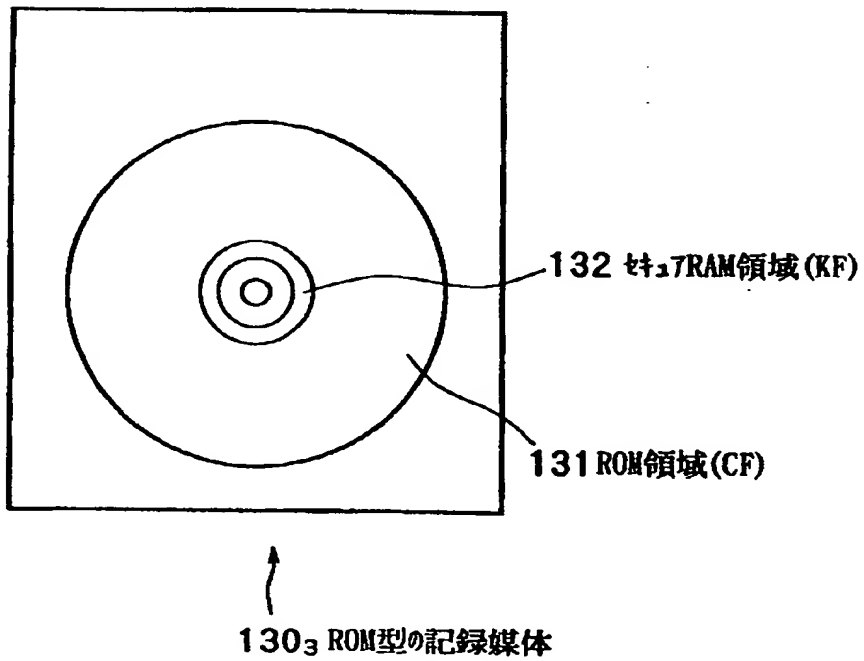


出証特２０００－３０８５０１６

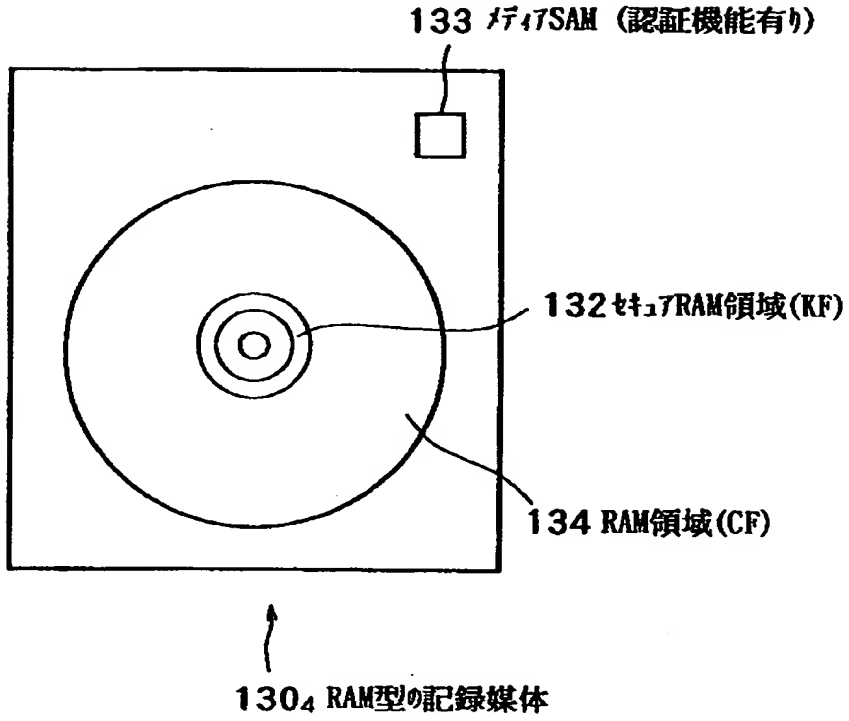
【図１２】


133 メディアSAM (・認証機能有り ・KF)
131 ROM領域(CF)
130₂ ROM型の記録媒体

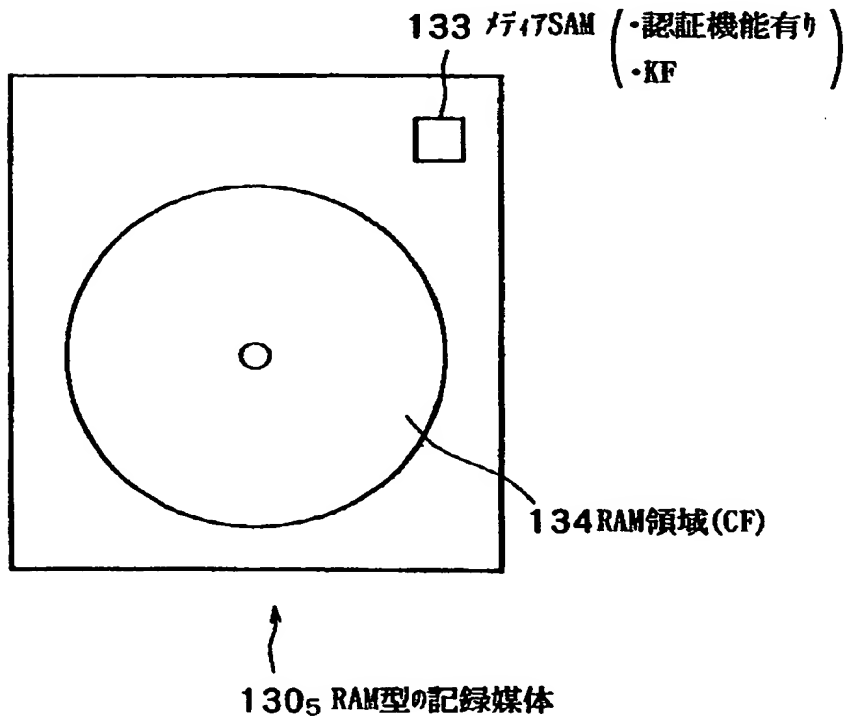
【図１３】


132 セキュアRAM領域(KF)
131 ROM領域(CF)
130₃ ROM型の記録媒体

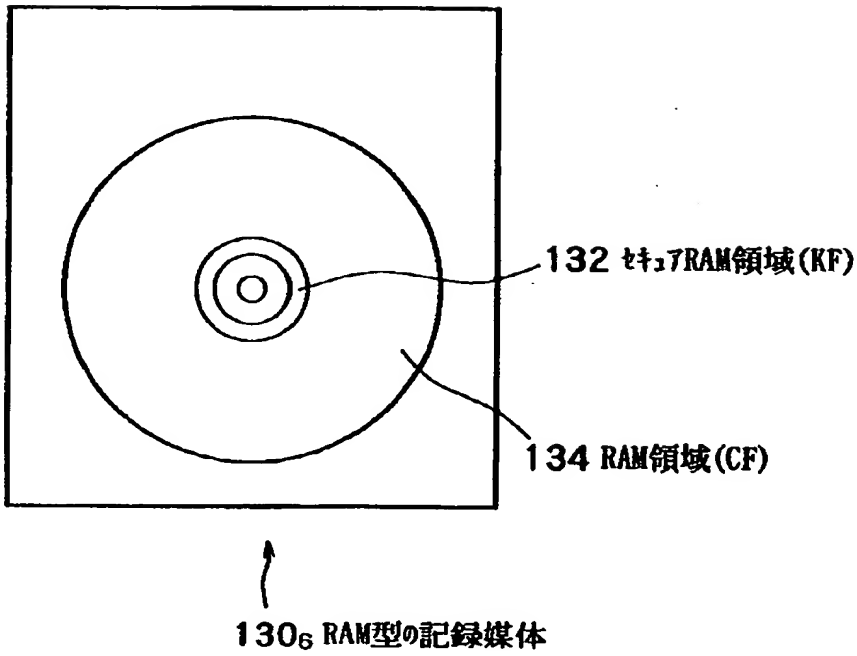
【図１４】


133 メディアSAM（認証機能有り）
132 セキュアRAM領域(KF)
134 RAM領域(CF)
130_4 RAM型の記録媒体

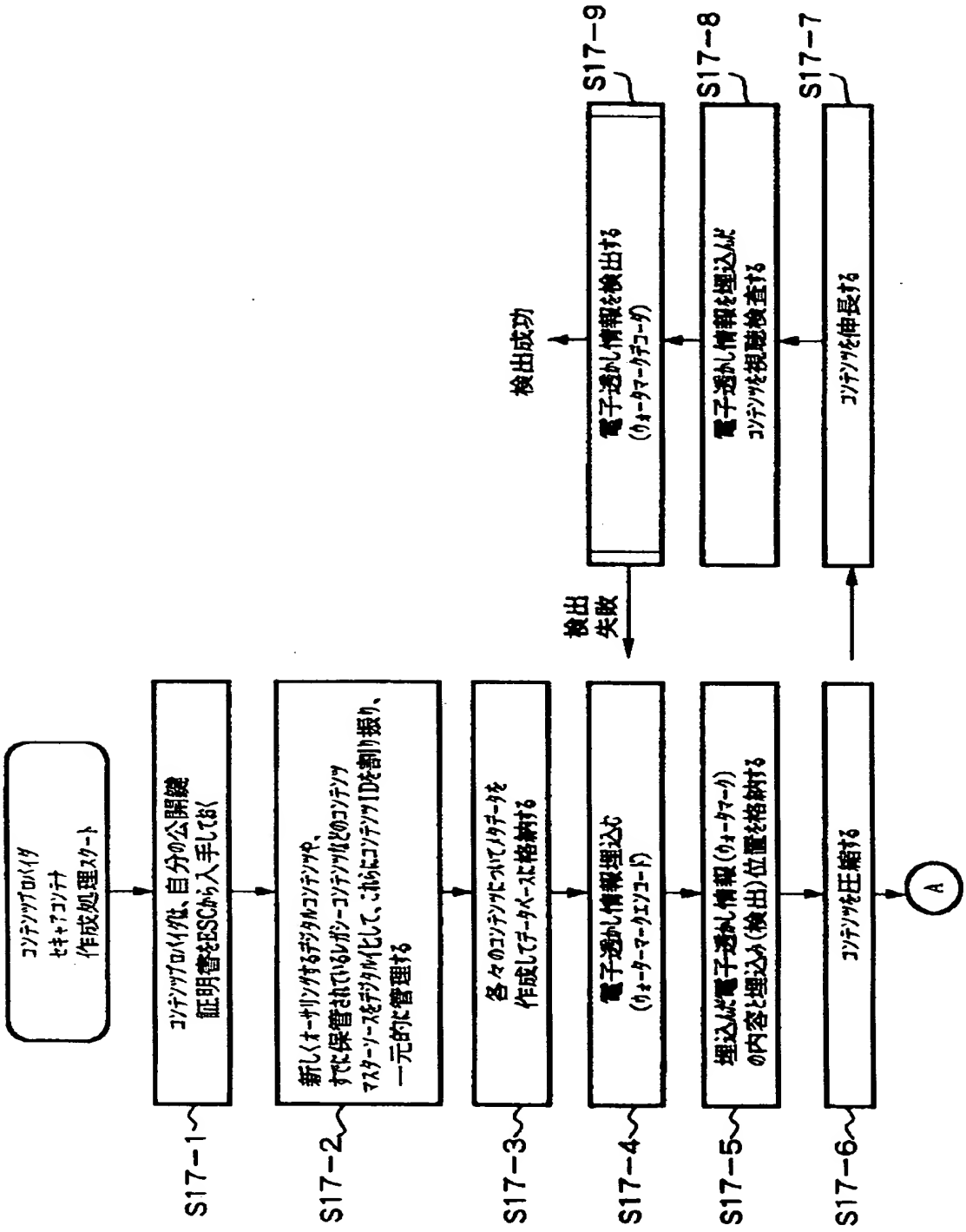
【図１５】


133 メディアSAM
・認証機能有り
・KF
134 RAM領域(CF)
130_5 RAM型の記録媒体

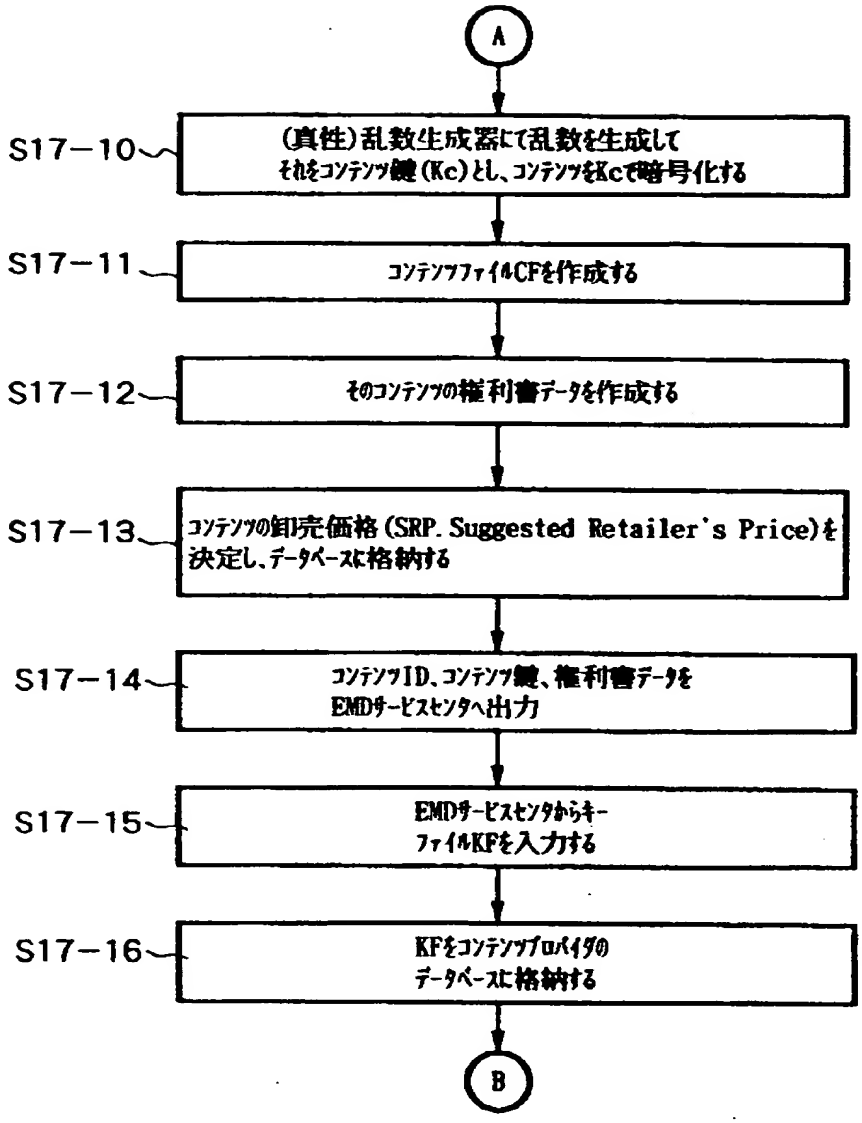
【図１６】



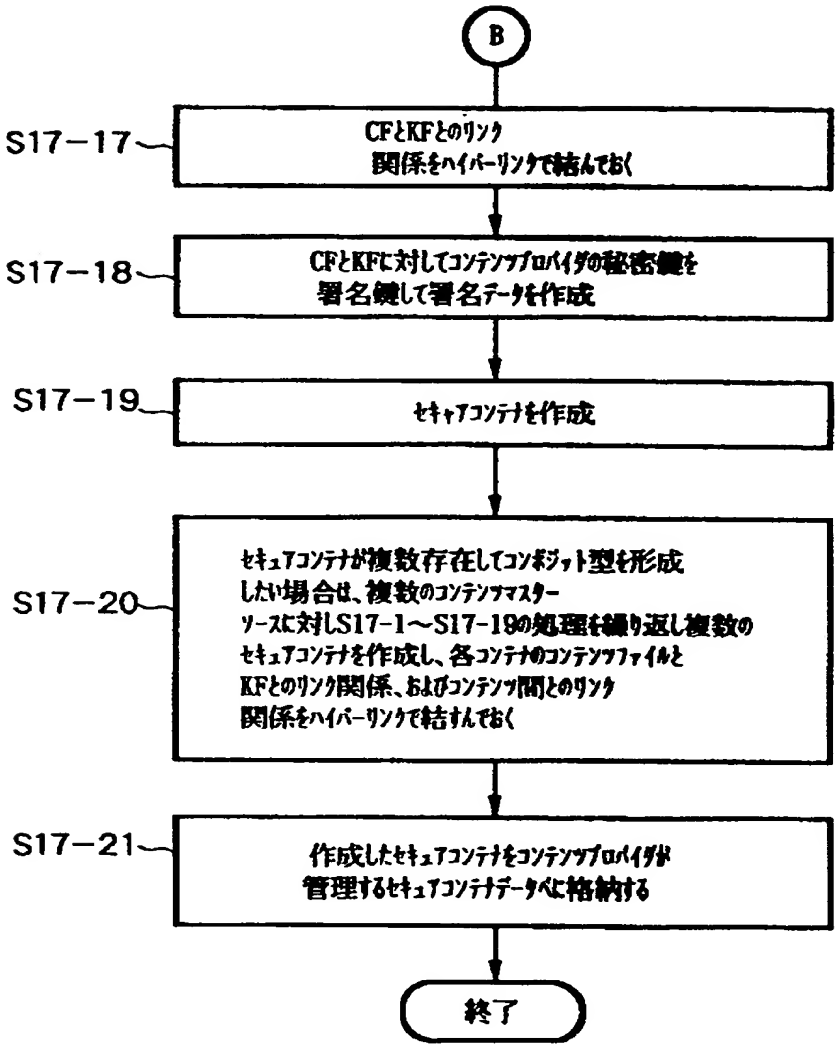
【図１７】


コンテンツプロバイダ
セキュアコンテナ
作成処理スタート
コンテンツプロバイダ他、自分の公開鍵
証明書をESCから入手しておく
新しくオーサリングするデジタルコンテンツや、
すでに保管されているレガシーコンテンツなどのコンテンツ
マスターソースをデジタル化して、これらにコンテンツIDを割り振り、
一元的に管理する
各々のコンテンツについてメタデータを
作成してデータベースに格納する
電子透かし情報埋込み
(ウォーターマークエンコード)
埋込んだ電子透かし情報(ウォーターマーク)
の内容と埋込み(検出)位置を格納する
コンテンツを圧縮する
A
S17-1
S17-2
S17-3
S17-4
S17-5
S17-6
検出成功
検出失敗
電子透かし情報を検出する
(ウォーターマークデコード)
電子透かし情報を埋込んだ
コンテンツを視聴検査する
コンテンツを伸長する
S17-9
S17-8
S17-7

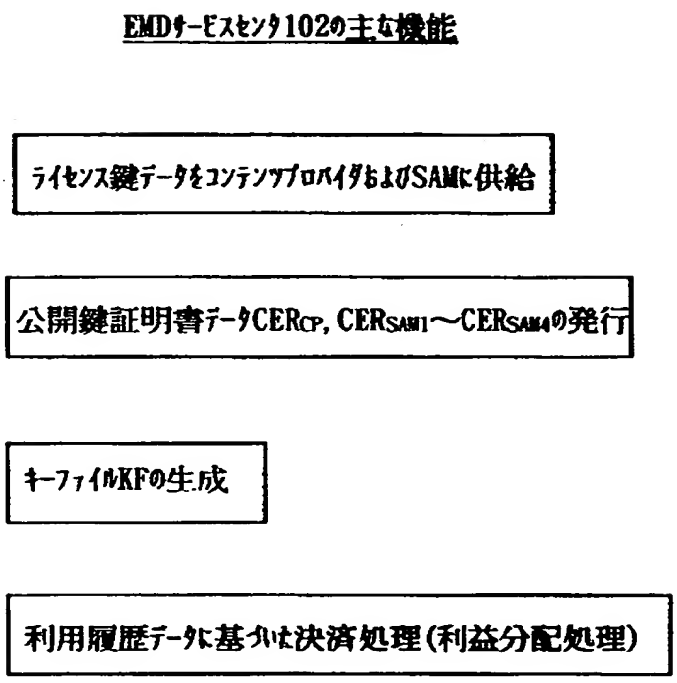
【図１８】


A
S17－10
(真性)乱数生成器にて乱数を生成して
それをコンテンツ鍵(Kc)とし、コンテンツをKcで暗号化する
S17－11
コンテンツファイルCFを作成する
S17－12
そのコンテンツの権利書データを作成する
S17－13
コンテンツの卸売価格(SRP. Suggested Retailer's Price)を
決定し、データベースに格納する
S17－14
コンテンツID、コンテンツ鍵、権利書データを
EMDサービスセンタへ出力
S17－15
EMDサービスセンタからキー
ファイルKFを入力する
S17－16
KFをコンテンツプロバイダの
データベースに格納する
B

【図１９】


B
S17-17
CFとKFとのリンク
関係をハイパーリンクで結んでおく
S17-18
CFとKFに対してコンテンツプロバイダの秘密鍵を
署名鍵して署名データを作成
S17-19
セキュアコンテナを作成
S17-20
セキュアコンテナが複数存在してコンポジット型を形成
したい場合は、複数のコンテンツマスター
ソースに対しS17-1～S17-19の処理を繰り返し複数の
セキュアコンテナを作成し、各コンテナのコンテンツファイルと
KFとのリンク関係、およびコンテンツ間とのリンク
関係をハイパーリンクで結んでおく
S17-21
作成したセキュアコンテナをコンテンツプロバイダが
管理するセキュアコンテナデータベに格納する
終了

【図２０】

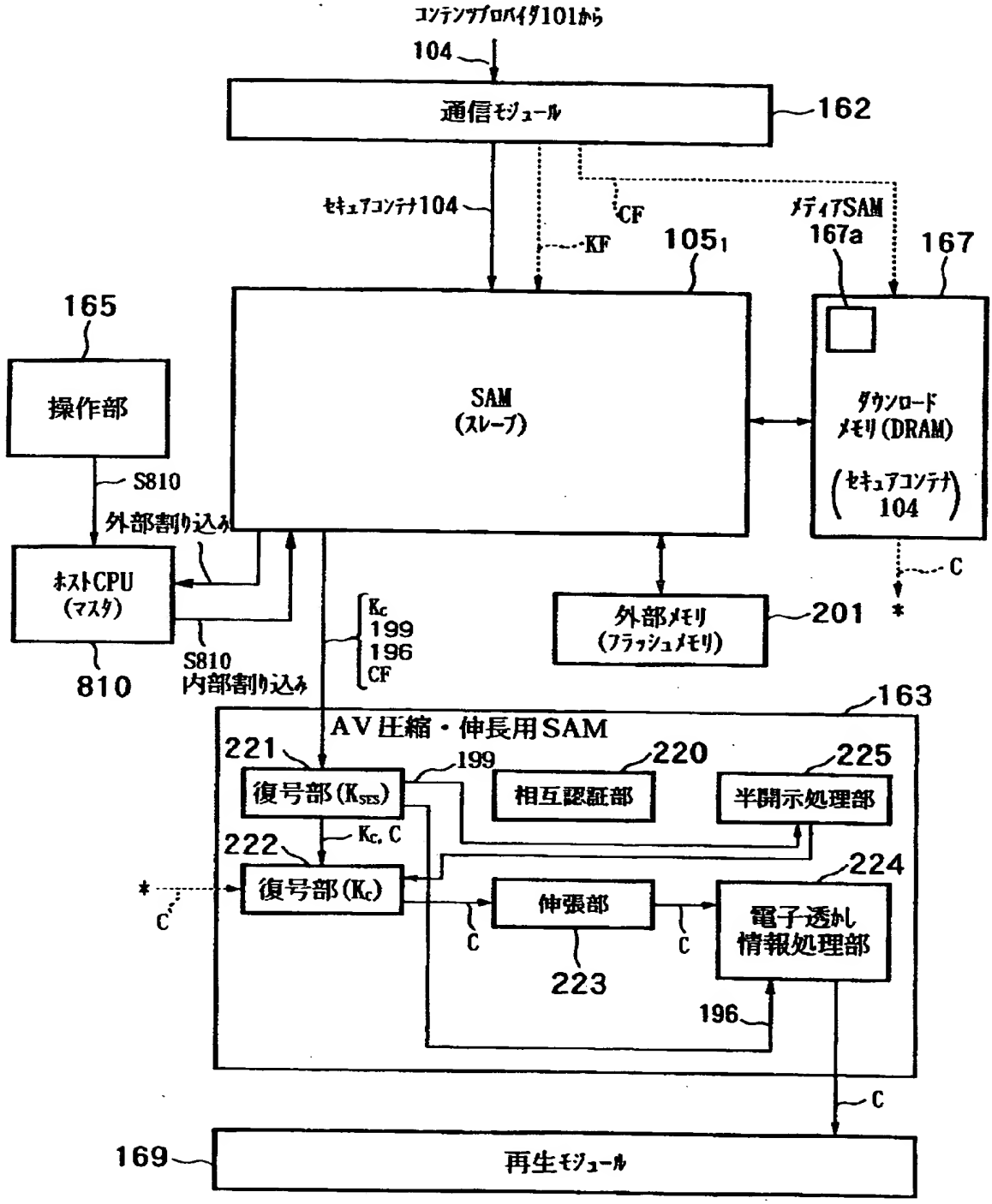

EMDサービスセンタ102の主な機能
ライセンス鍵データをコンテンツプロバイダおよびSAMに供給
公開鍵証明書データCERCP, CERSAM1～CERSAM4の発行
キーファイルKFの生成
利用履歴データに基づいた決済処理(利益分配処理)

【図２１】

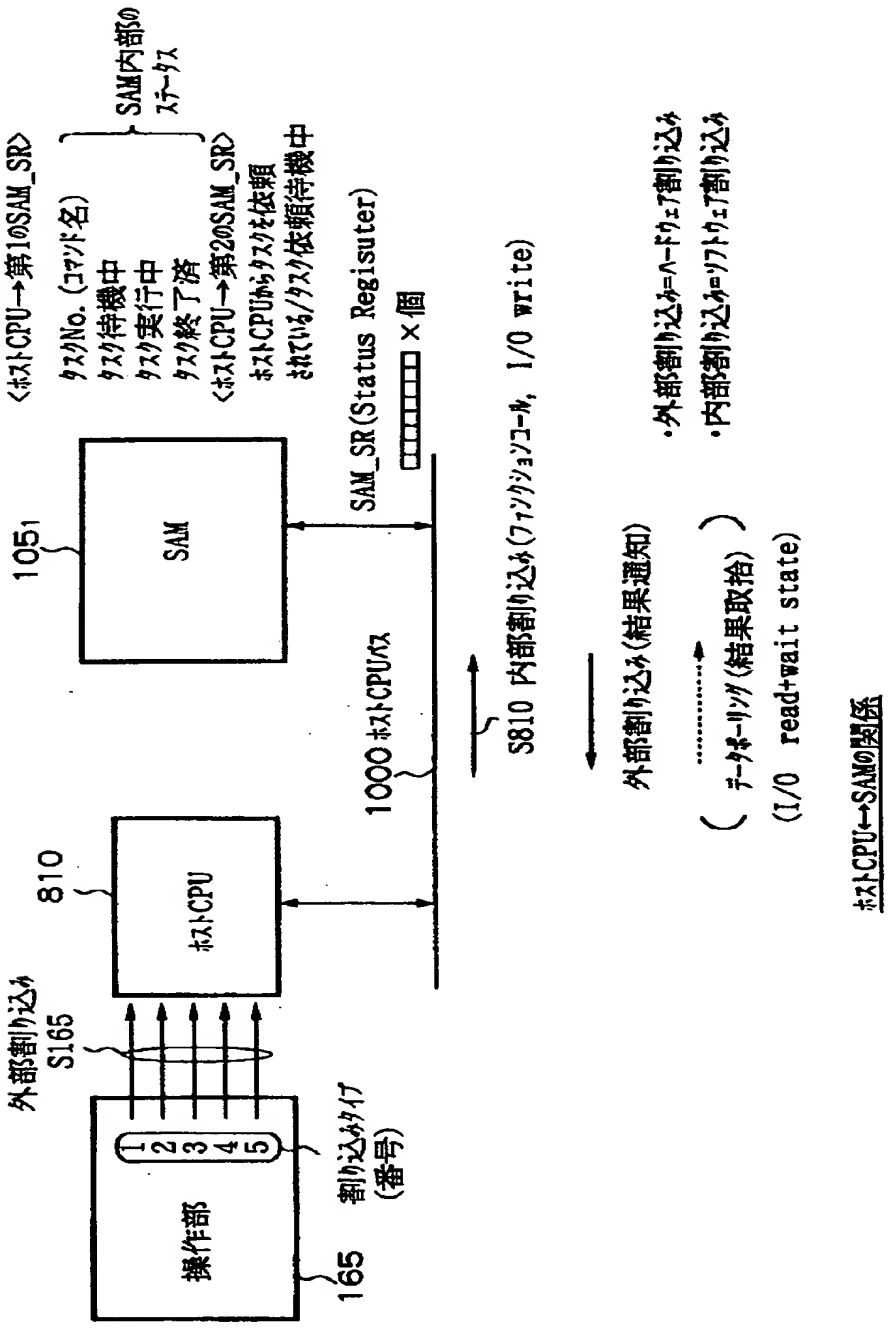
利用履歴ﾃﾞｰﾀ108(308)

ESC_ｺﾝﾃﾝﾂID
CP_ｺﾝﾃﾝﾂID
(SP_ｺﾝﾃﾝﾂID)
ﾕｰｻﾞID
ﾕｰｻﾞ情報
SAM_ID
HNG_ID
ﾃｨｽｶｳﾝﾄ情報
ﾄﾚｰｼﾝｸﾞ情報
(ﾌﾟﾗｲｽﾀｸﾞﾃﾞｰﾀPT)
CP_ID
(SP_ID)
紹介業者(ﾎﾟｰﾀﾙ:Portal)ID
ﾊｰﾄﾞｳｪｱ提供者ID
Media_ID
ｺﾝﾎﾟｰﾈﾝﾄID
ﾗｲｾﾝｽ所有者の識別子LH_ID
ESC_ID

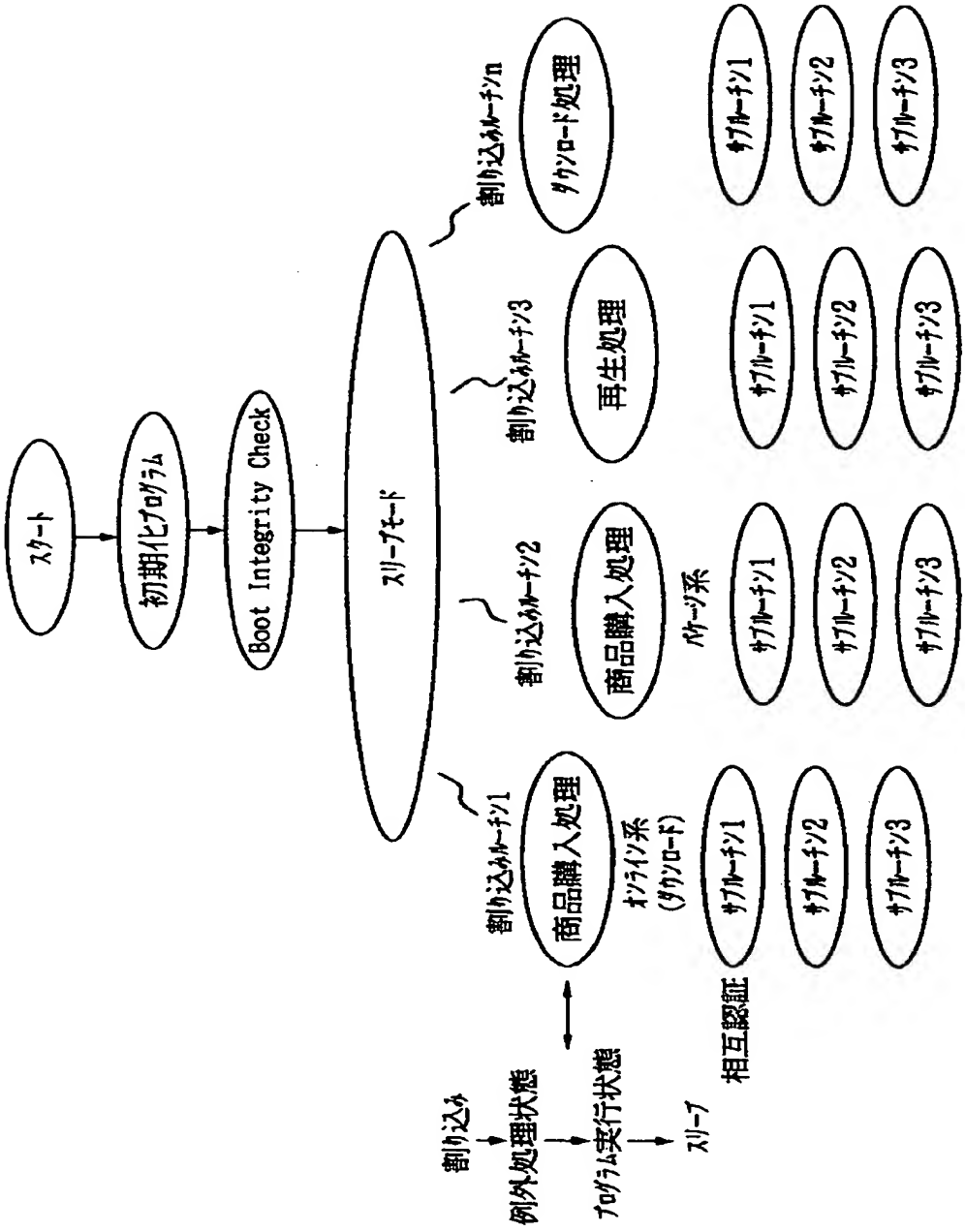
【図２２】


コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
CF
KF
105₁
メディアSAM
167a
167
165
操作部
SAM
(スレーブ)
ダウンロード
メモリ(DRAM)
(セキュアコンテナ
104)
S810
外部割り込み
ホストCPU
(マスタ)
Kc
199
196
CF
外部メモリ
(フラッシュメモリ)
201
C
*
S810
内部割り込み
810
163
AV圧縮・伸長用SAM
221
199
220
225
復号部(Kses)
相互認証部
半開示処理部
Kc, C
222
224
*
C
復号部(Kc)
伸張部
電子透かし
情報処理部
C
C
223
196
C
169
再生モジュール

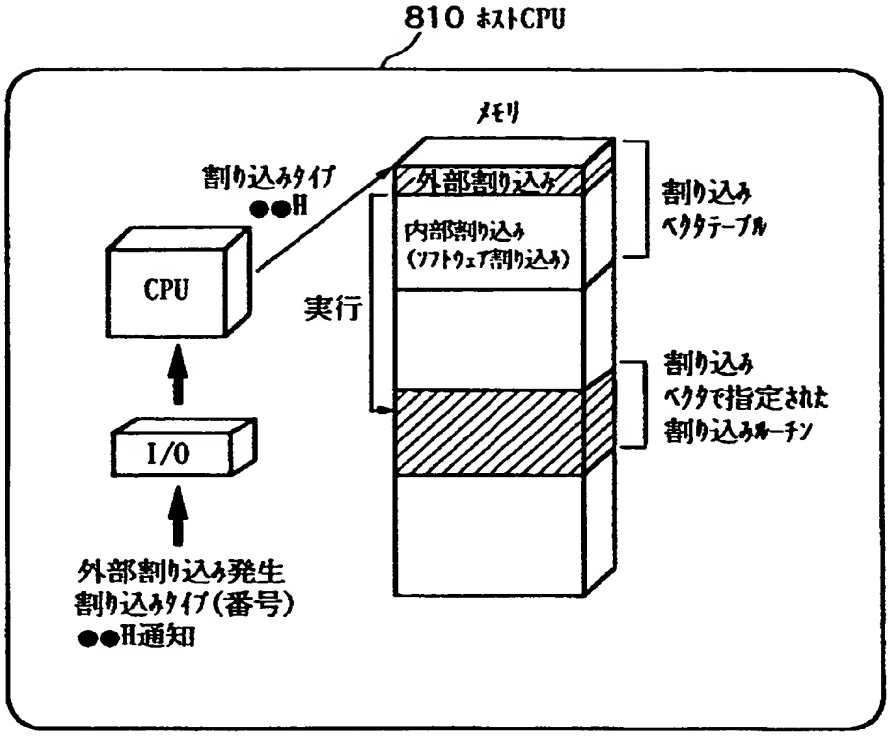
【図２３】


外部割り込み
S165
810
ホストCPU
1000 ホストCPUバス
1051
SAM
SAM_SR(Status Regisuter)
×個
S810 内部割り込み(ファンクションコール, I/O write)
外部割り込み(結果通知)
(I/O read+wait state)
ホストCPU↔SAMの関係
操作部
165
割り込みタイプ
(番号)
1
2
3
4
5
<ホストCPU→第1のSAM_SR>
タスクNo.(コマンド名)
タスク待機中
タスク実行中
タスク終了済
<ホストCPU→第2のSAM_SR>
ホストCPUからタスクを依頼
されている/タスク依頼待機中
SAM内部の
ステータス
・外部割り込み=ハードウェア割り込み
・内部割り込み=ソフトウェア割り込み
データキーリング(結果取得)

【図２４】

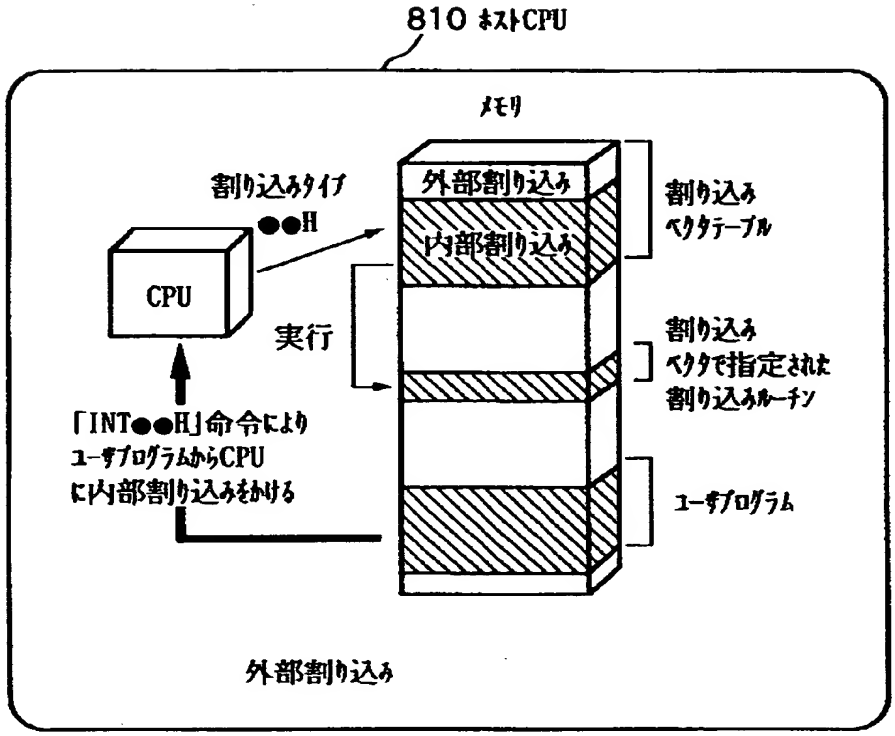

スタート
初期化プログラム
Boot Integrity Check
スリープモード
割り込みルーチン1
商品購入処理
オンライン系
(ダウンロード)
サブルーチン1
サブルーチン2
サブルーチン3
割り込みルーチン2
商品購入処理
バーツ系
サブルーチン1
サブルーチン2
サブルーチン3
割り込みルーチン3
再生処理
サブルーチン1
サブルーチン2
サブルーチン3
割り込みルーチンn
ダウンロード処理
サブルーチン1
サブルーチン2
サブルーチン3
割り込み
例外処理状態
プログラム実行状態
スリープ
相互認証

【図２５】



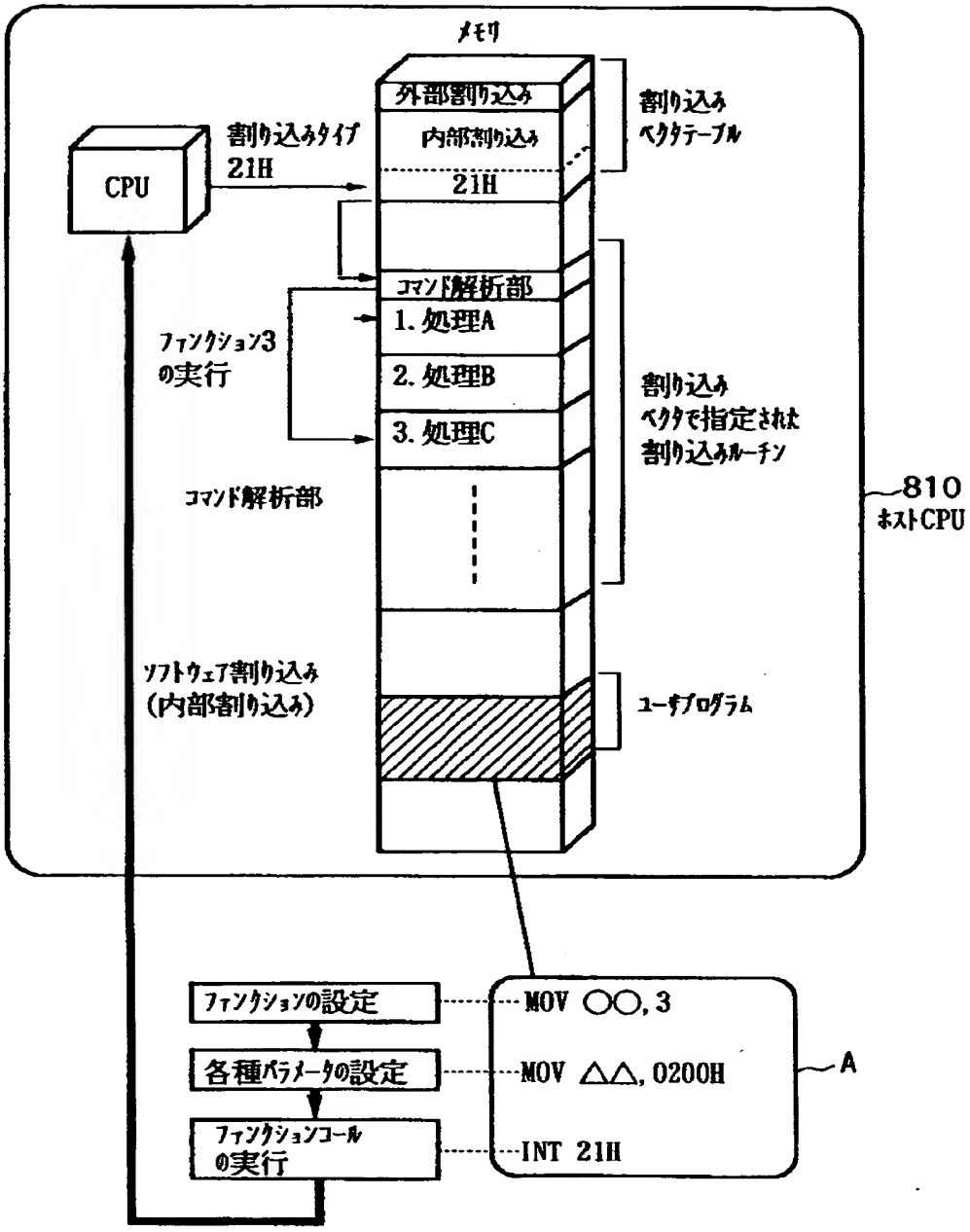
ハードウェア割り込み(外部割り込み)

【図２６】



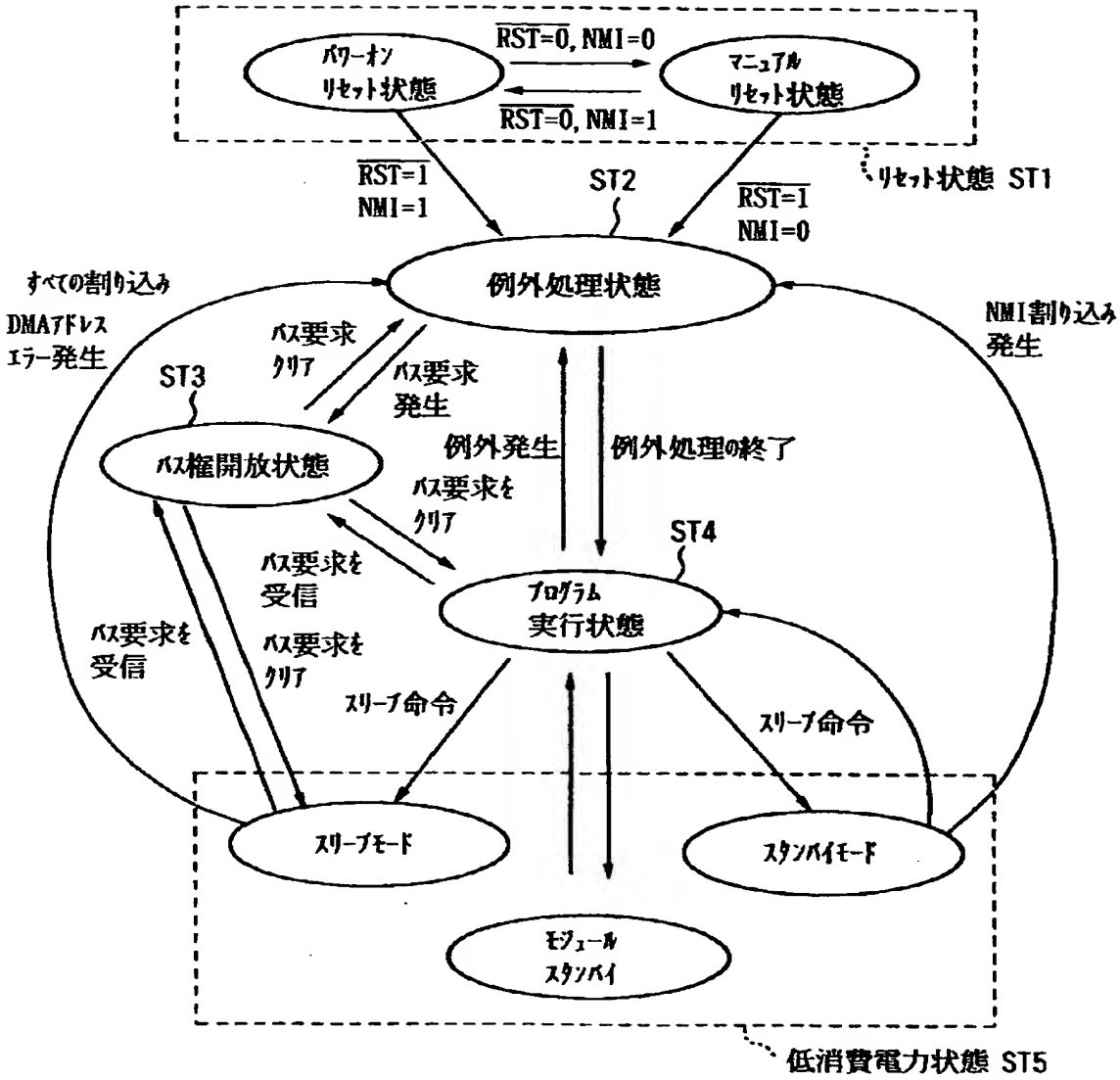
ソフトウェア割り込み(内部割り込み)

【図２７】



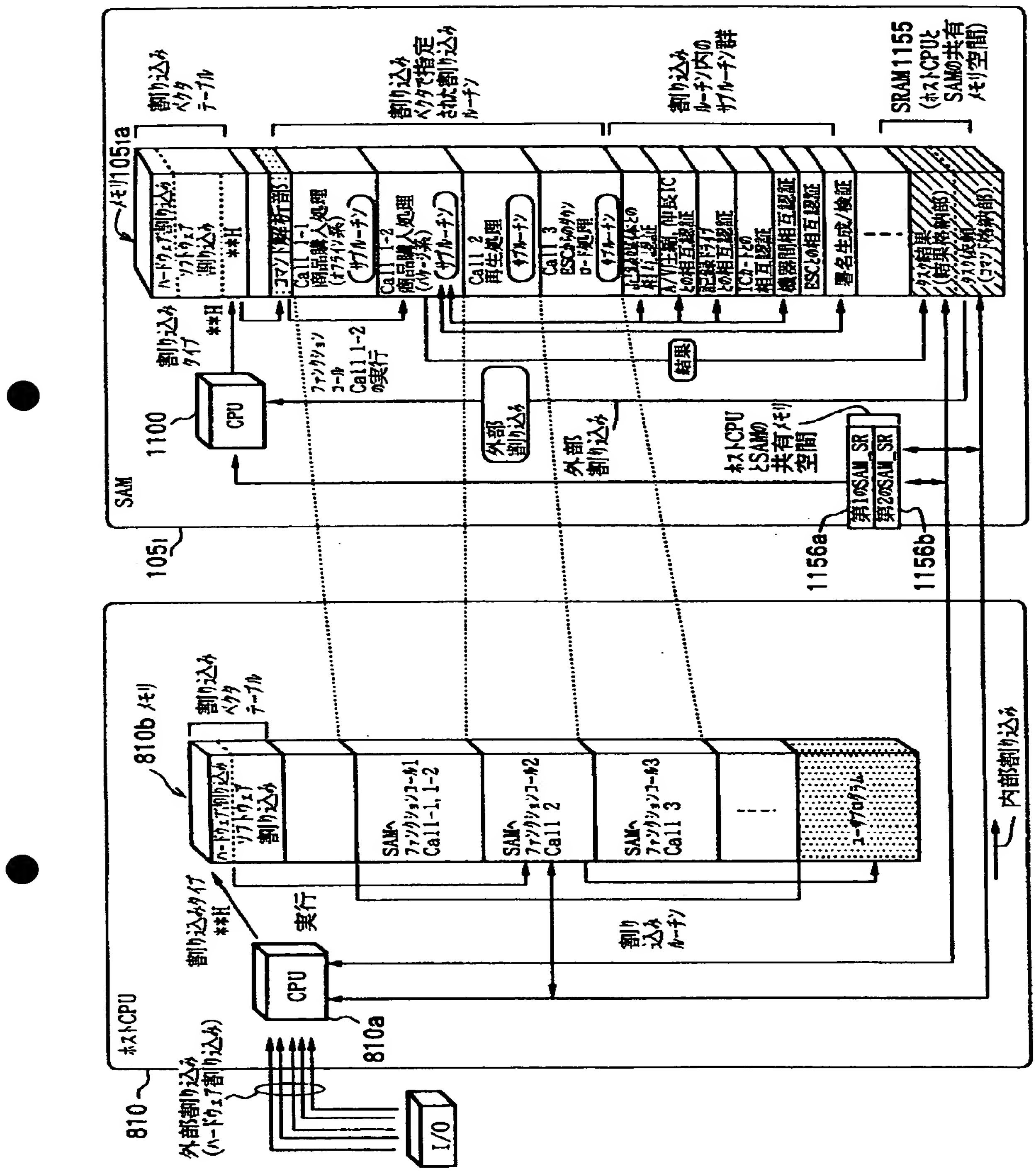
ファンクションコール(Procedure Call)

【図２８】

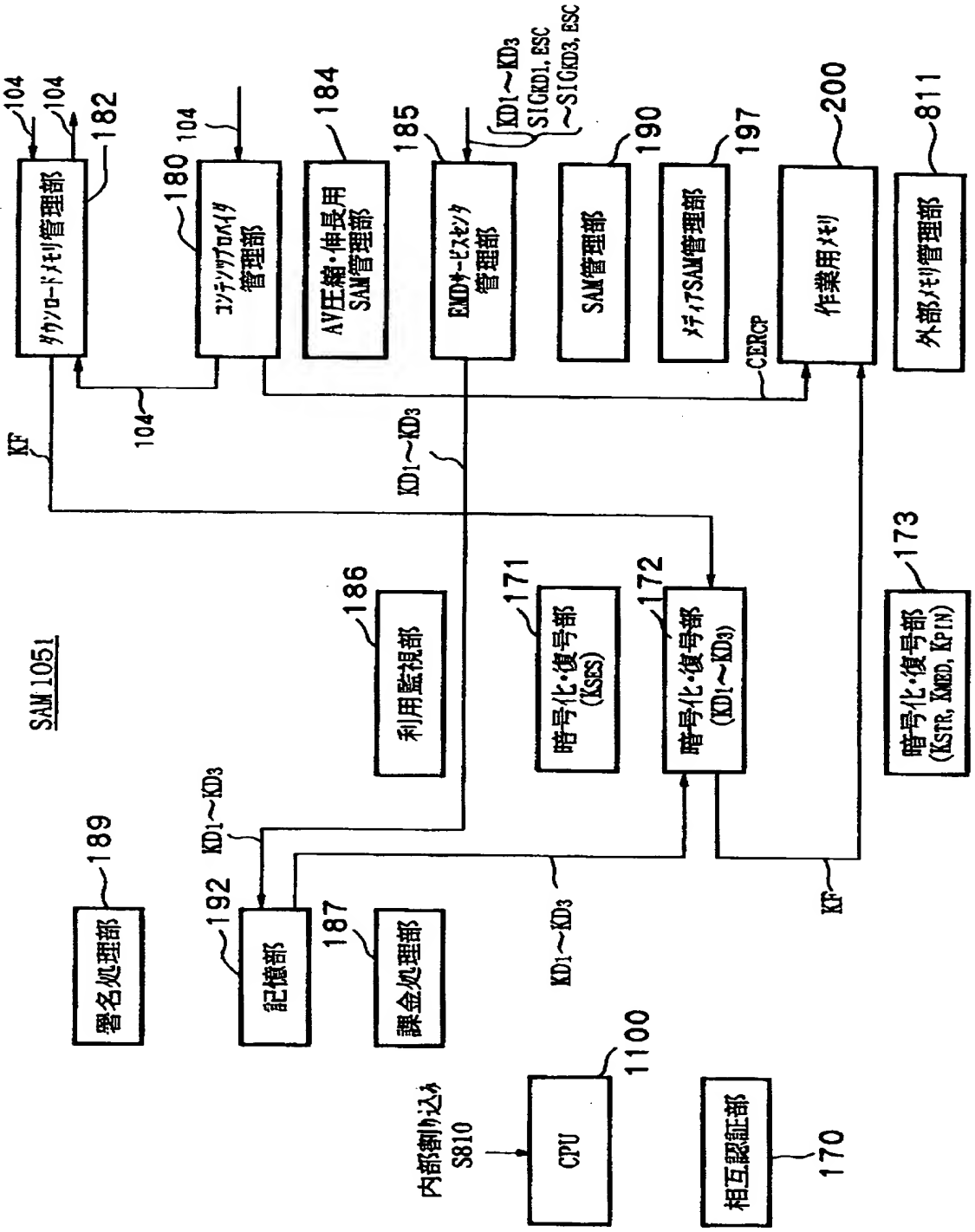


SAMのCPUの処理状態

【図２９】


SAM
1051
メモリ1051a
割り込みベクタテーブル
ハードウェア割り込み
ソフトウェア割り込み
**H
割り込みで指定された割り込みルーチン
割り込みルーチン内のサブルーチン群
SRAM1155
(ホストCPUとSAMの共有メモリ空間)
コマンド解析部
Call 1-1
商品購入処理
(オフライン系)
サブルーチン
Call 1-2
商品購入処理
Call 2
再生処理
Call 3
ESCからのダウンロード処理
A/Vとの相互認証
記録ドライブとの相互認証
機器間相互認証
ESCとの相互認証
署名生成/検証
タスク結果
タスク依頼
割り込みタイプ
**H
ファンクションコール
Call 1-2
の実行
結果
外部割り込み
1100
CPU
ホストCPUとSAMの共有メモリ空間
第1のSAM_SR
第2のSAM_SR
1156a
1156b
ホストCPU
810
810a
810b メモリ
割り込みベクタテーブル
ハードウェア割り込み
ソフトウェア割り込み
SAMへファンクションコール1
Call 1-1, 1-2
SAMへファンクションコール2
Call 2
SAMへファンクションコール3
Call 3
ユーザプログラム
割り込みタイプ
**H
実行
割り込みルーチン
内部割り込み
外部割り込み
(ハードウェア割り込み)
I/O

【図３０】


SAM 1051
ダウンロードメモリ管理部
182
104
エンティタプロバイダ管理部
180
AV圧縮・伸長用SAM管理部
184
EMDサービスセンタ管理部
185
SAM管理部
190
メディアSAM管理部
197
作業用メモリ
200
外部メモリ管理部
811
KD1～KD3
SIGKD1, ESC
～SIGKD3, ESC
CERCP
KF
利用監視部
186
暗号化・復号部 (KSCS)
171
暗号化・復号部 (KD1～KD3)
172
暗号化・復号部 (KSTR, KMED, KPIN)
173
署名処理部
189
記憶部
192
課金処理部
187
CPU
1100
相互認証部
170
内部割り込み
S810

【図３１】

外部メモリ201に記憶されるデータ

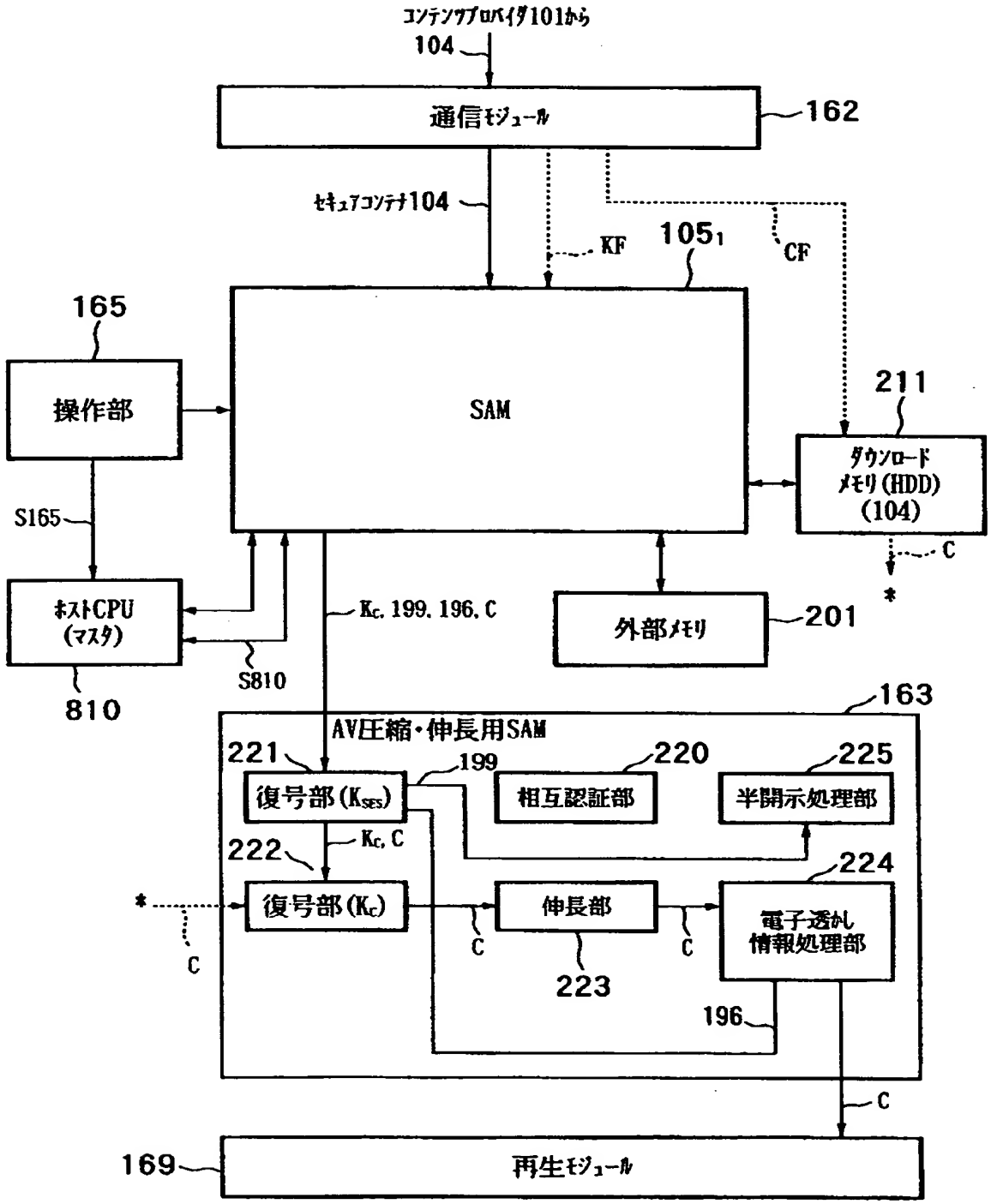
利用履歴データ108
SAM登録リスト
(KF:ダウンロードメモリにメディアSAMが無い場合)

【図３２】

作業用メモリ200に記憶されるデータ

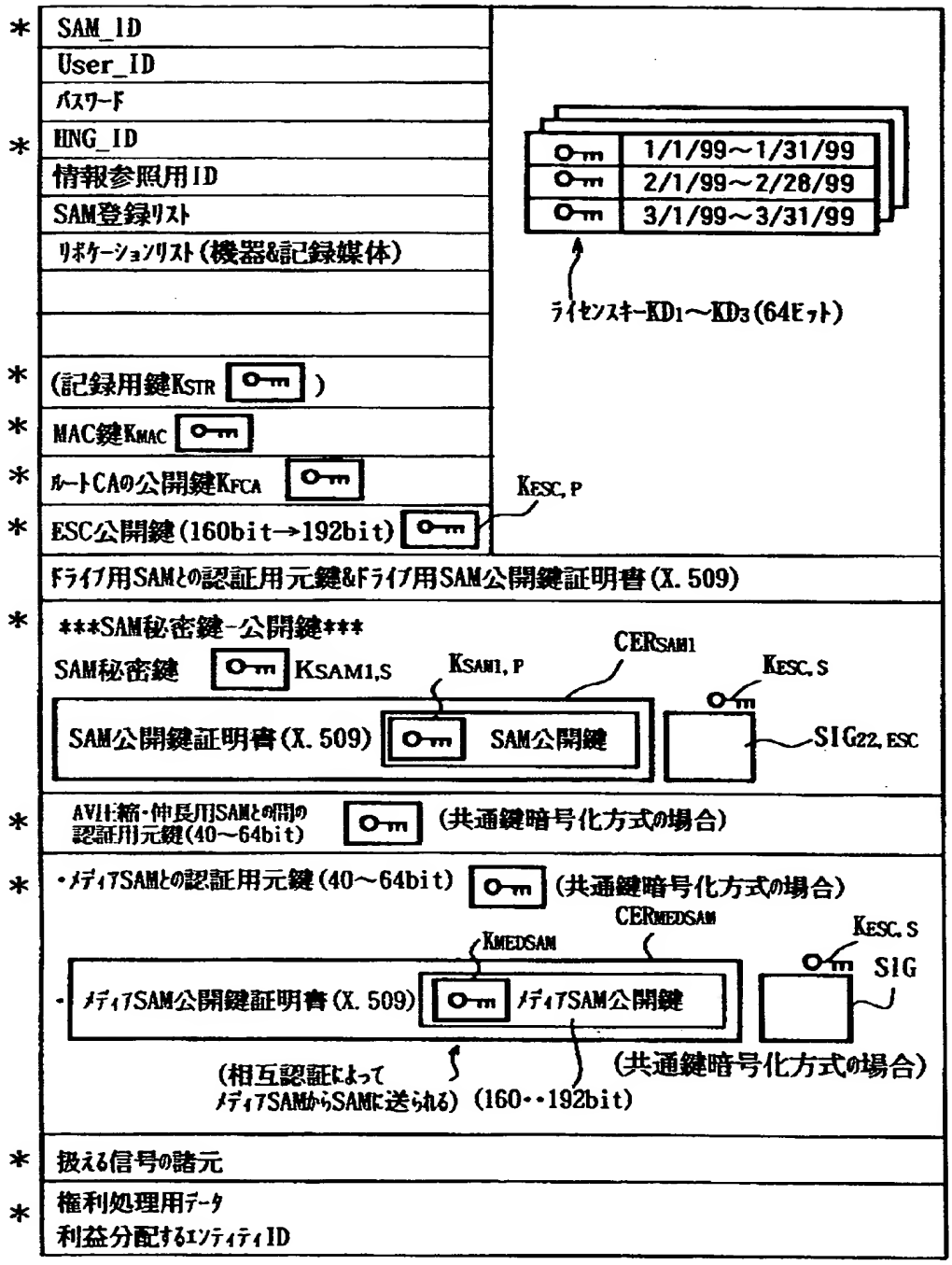
コンテンツ鍵データK_C
権利書データ(UCP)106
記憶部(フラッシュメモリ)192のロック鍵データK_{LOC}
コンテンツプロバイダ101の公開鍵証明書CER_{CP}
利用制御データ(UCS)166
SAMプログラム・ダウンロード・コンテナSD_1～SDC_3

【図３３】

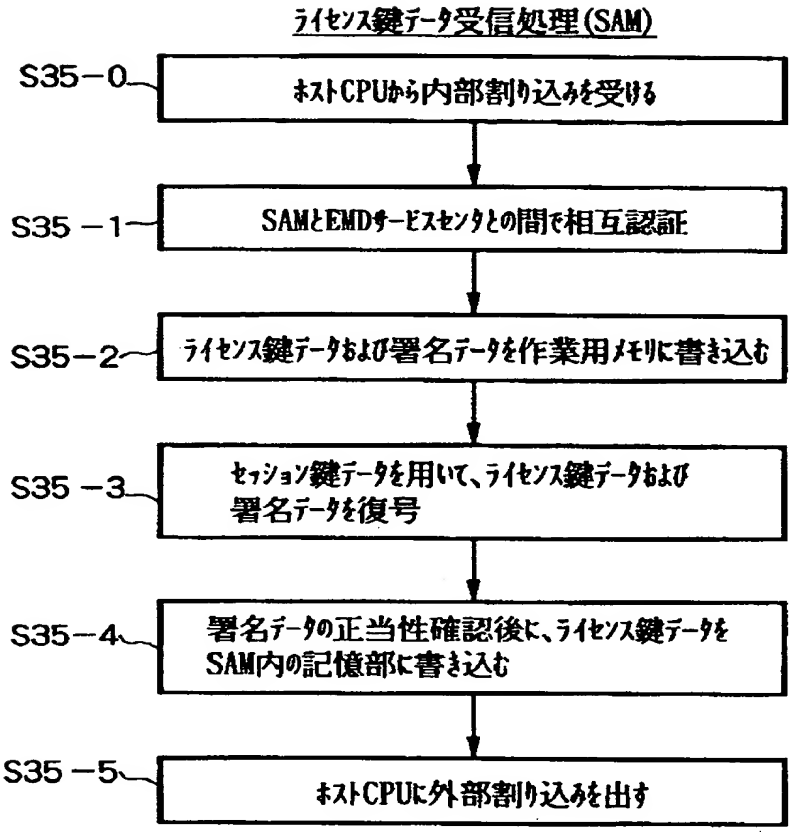

コンテンツプロバイダ101から
104
通信モジュール
162
セキュアコンテナ104
KF
105₁
CF
165
操作部
SAM
211
ダウンロード
メモリ(HDD)
(104)
C
*
S165
ホストCPU
(マスタ)
810
S810
Kc, 199, 196, C
外部メモリ
201
163
AV圧縮・伸長用SAM
221
199
220
225
復号部(Kses)
相互認証部
半開示処理部
222
Kc, C
224
*
復号部(Kc)
伸長部
電子透かし
情報処理部
C
C
C
223
196
C
169
再生モジュール

【図３４】

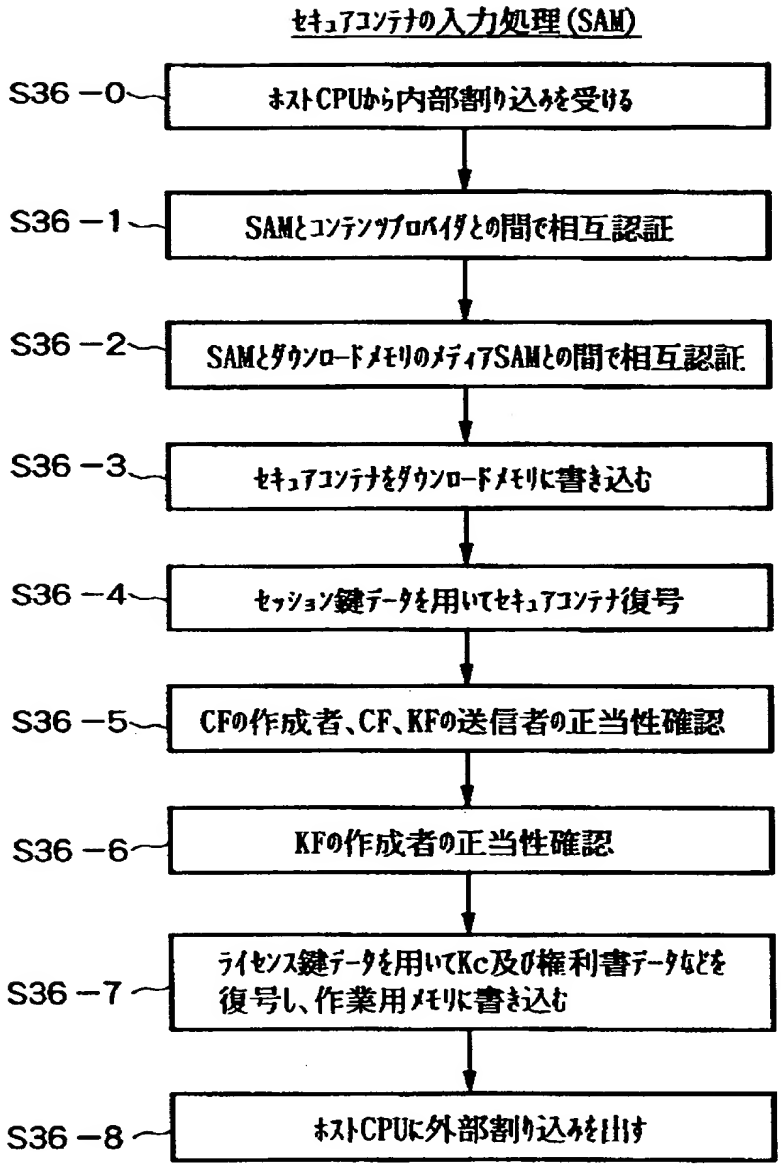
記憶部192に記憶されるデータ



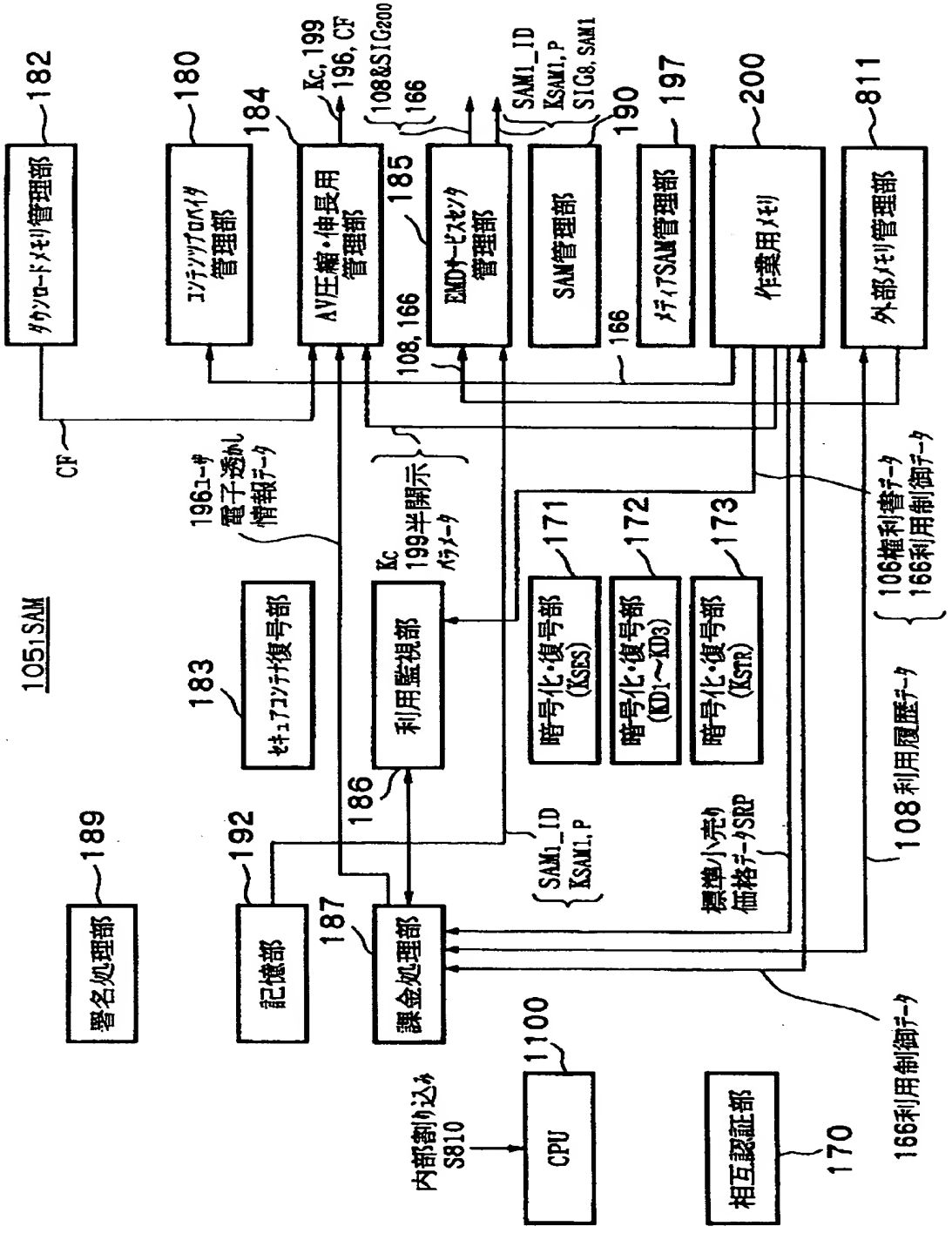
【図３５】


ライセンス鍵データ受信処理(SAM)
S35－0
ホストCPUから内部割り込みを受ける
S35－1
SAMとEMDサービスセンタとの間で相互認証
S35－2
ライセンス鍵データおよび署名データを作業用メモリに書き込む
S35－3
セッション鍵データを用いて、ライセンス鍵データおよび署名データを復号
S35－4
署名データの正当性確認後に、ライセンス鍵データをSAM内の記憶部に書き込む
S35－5
ホストCPUに外部割り込みを出す

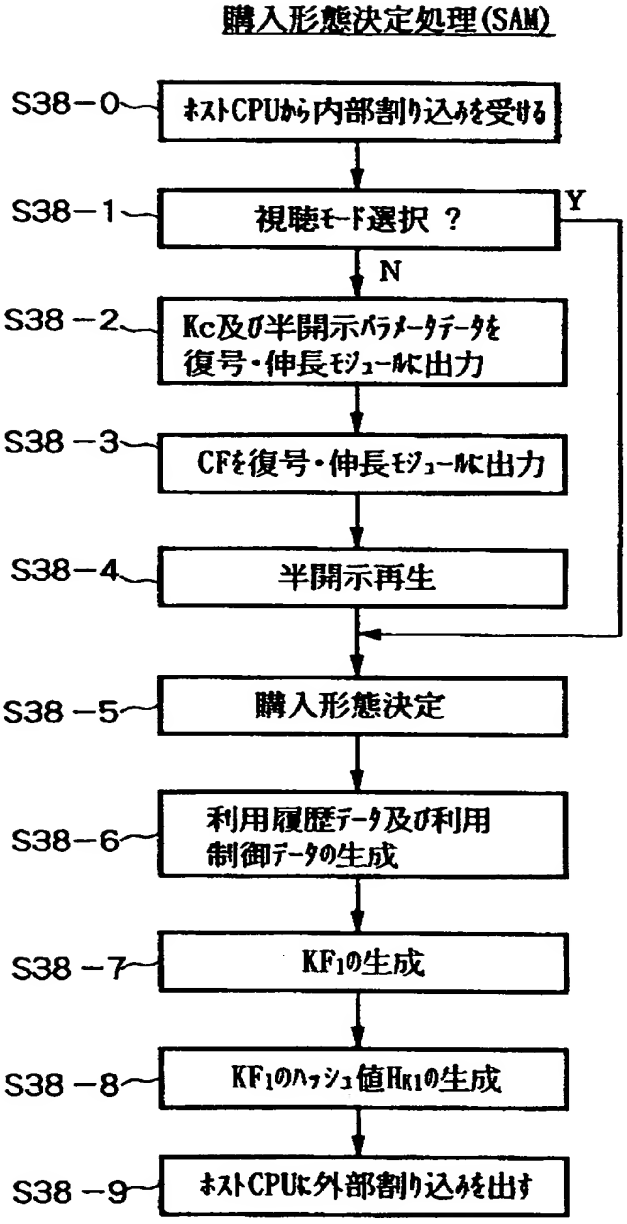
【図３６】


セキュアコンテナの入力処理(SAM)
S36－0
ホストCPUから内部割り込みを受ける
S36－1
SAMとコンテンツプロバイダとの間で相互認証
S36－2
SAMとダウンロードメモリのメディアSAMとの間で相互認証
S36－3
セキュアコンテナをダウンロードメモリに書き込む
S36－4
セッション鍵データを用いてセキュアコンテナ復号
S36－5
CFの作成者、CF、KFの送信者の正当性確認
S36－6
KFの作成者の正当性確認
S36－7
ライセンス鍵データを用いてKc及び権利書データなどを復号し、作業用メモリに書き込む
S36－8
ホストCPUに外部割り込みを出す

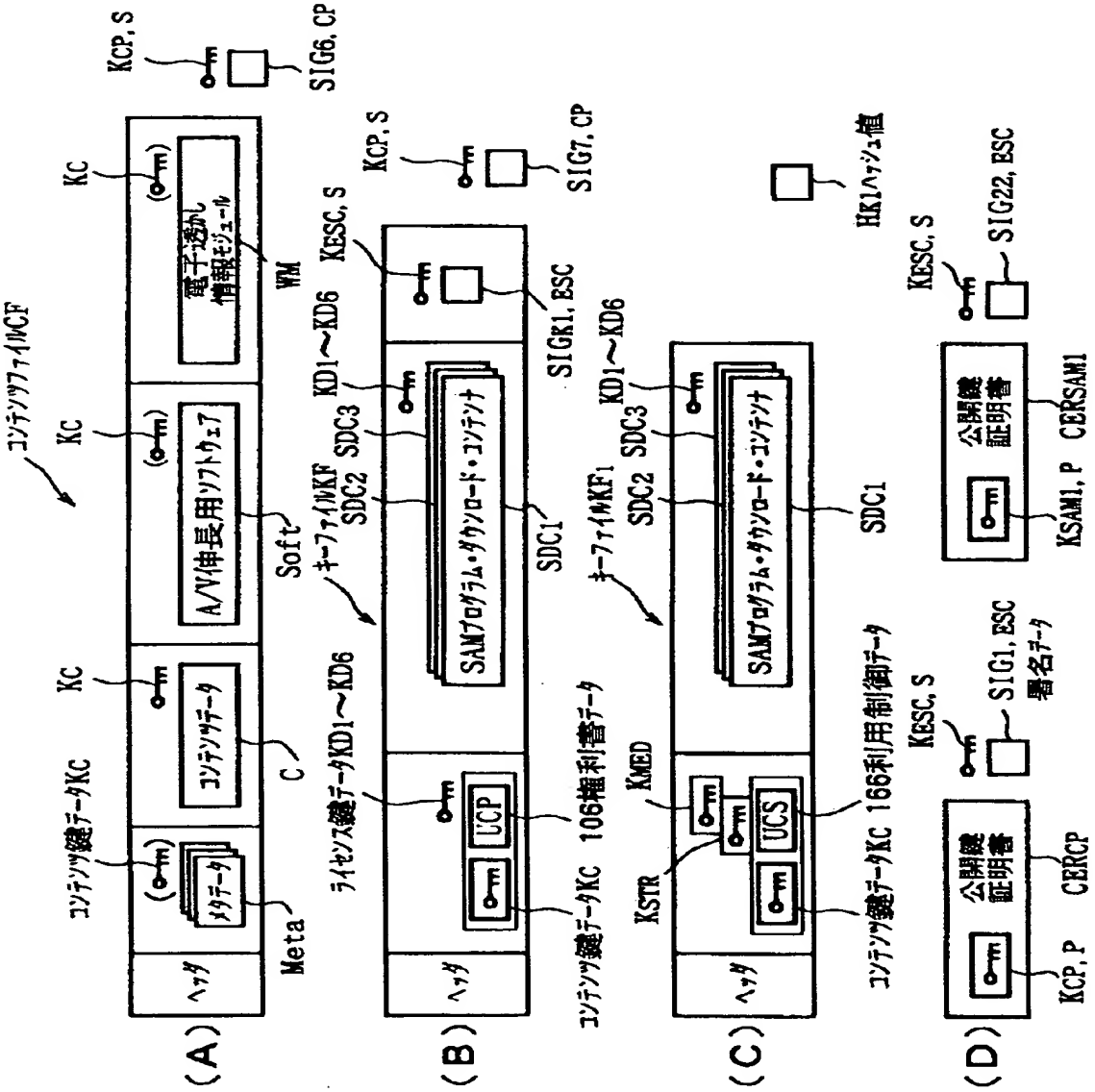
【図３７】


182
ダウンロードメモリ管理部
180
コンテンツプロバイダ管理部
184
Kc, 199
196, CF
AV圧縮・伸長用管理部
185
108&SIG200
166
EMDサービスセンタ管理部
SAM1_ID
KSAM1, P
SIG8, SAM1
190
SAM管理部
197
メディアSAM管理部
200
作業用メモリ
811
外部メモリ管理部
CF
196ユーザ電子透かし情報データ
108, 166
166
105 SAM
Kc
199半開示
パラメータ
183
セキュアコンテナ復号部
利用監視部
171
暗号化・復号部
(KSES)
172
暗号化・復号部
(KD1～KD3)
173
暗号化・復号部
(KSTR)
106権利書データ
166利用制御データ
189
署名処理部
192
記憶部
186
187
課金処理部
SAM1_ID
KSAM1, P
標準小売り価格データSRP
108利用履歴データ
166利用制御データ
1100
CPU
内部割り込み
S810
相互認証部
170

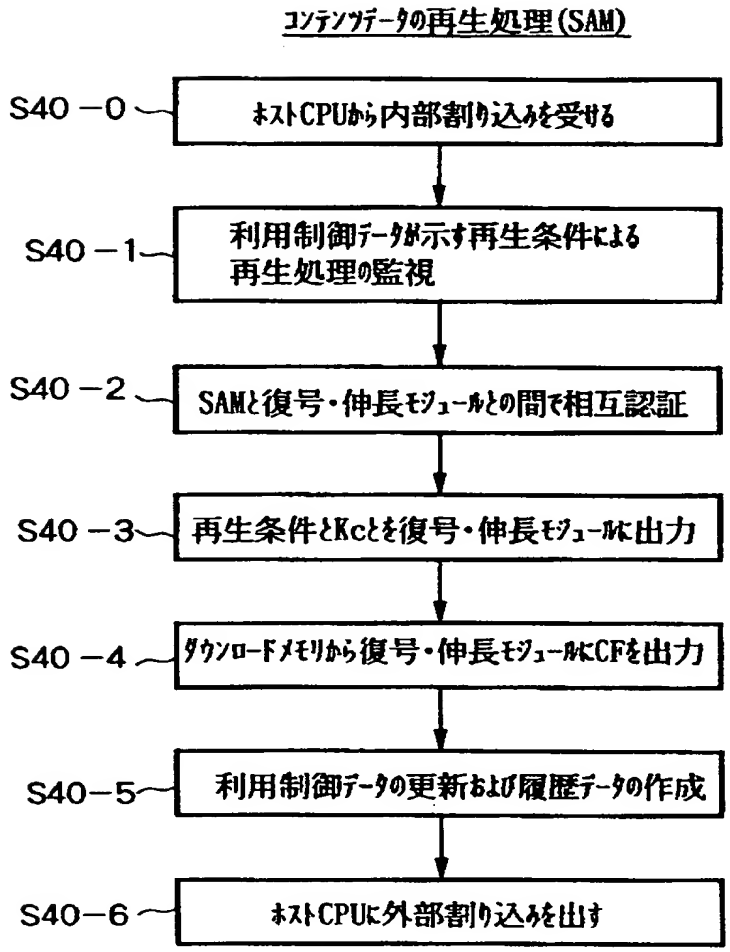
【図３８】


購入形態決定処理(SAM)
S38－0
ホストCPUから内部割り込みを受ける
S38－1
視聴モード選択 ？
Y
N
S38－2
Kc及び半開示パラメータデータを
復号・伸長モジュールに出力
S38－3
CFを復号・伸長モジュールに出力
S38－4
半開示再生
S38－5
購入形態決定
S38－6
利用履歴データ及び利用
制御データの生成
S38－7
KF1の生成
S38－8
KF1のハッシュ値HK1の生成
S38－9
ホストCPUに外部割り込みを出す

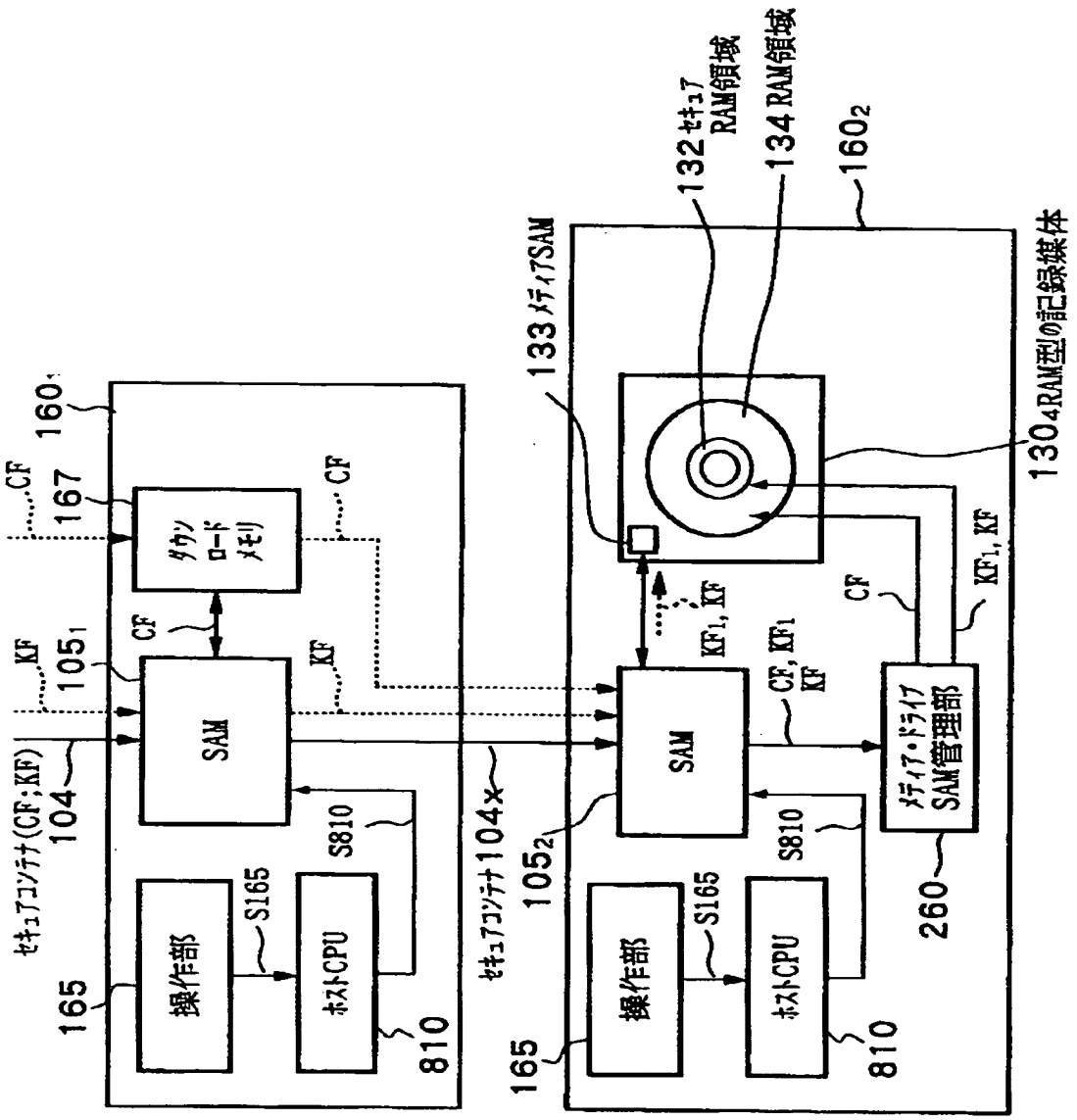
【図３９】


コンテンツファイルMCF
Kc
KCP, S
SIG6, CP
電子透かし情報モジュール
WM
A/V伸長用ソフトウェア
Soft
コンテンツデータ
C
メタデータ
Meta
コンテンツ鍵データKc
ヘッダ
(A)
ライセンス鍵データKD1～KD6
キーファイルMKF
SDC2
SDC3
KD1～KD6
KESC, S
SIGK1, ESC
SIG7, CP
SAMプログラム・ダウンロード・コンテンツ
SDC1
UCP
コンテンツ鍵データKc
106権利書データ
(B)
KMED
KSTR
UCS
166利用制御データ
HK1ハッシュ値
(C)
SIG22, ESC
公開鍵証明書
KSAM1, P
CERSAM1
SIG1, ESC
署名データ
KCP, P
CERCP
(D)

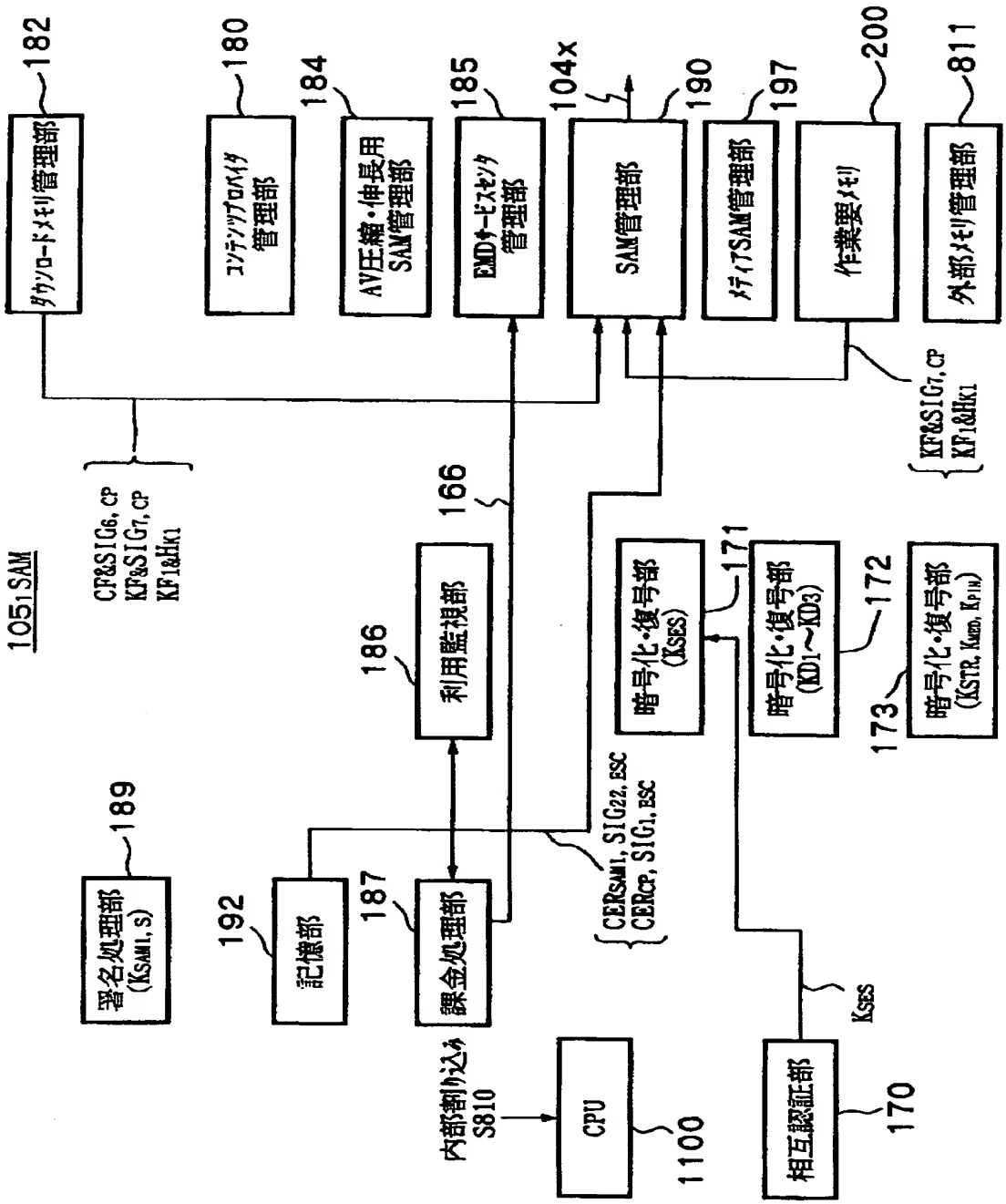
【図４０】


コンテンツデータの再生処理(SAM)
S40－0
ホストCPUから内部割り込みを受ける
S40－1
利用制御データが示す再生条件による
再生処理の監視
S40－2
SAMと復号・伸長モジュールとの間で相互認証
S40－3
再生条件とKcとを復号・伸長モジュールに出力
S40－4
ダウンロードメモリから復号・伸長モジュールにCFを出力
S40－5
利用制御データの更新および履歴データの作成
S40－6
ホストCPUに外部割り込みを出す

【図４１】

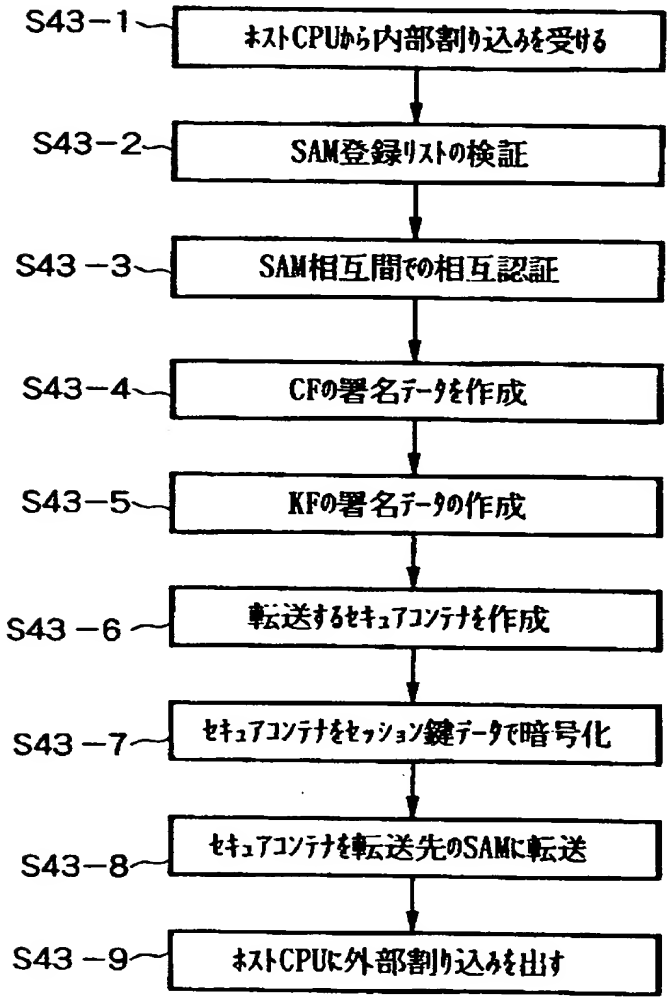

160
CF
167
ダウンロードメモリ
CF
KF
105₁
CF
KF
SAM
セキュアコンテナ(CF;KF)
104
S810
操作部
S165
ホストCPU
165
810
セキュアコンテナ104ₓ
133 メディアSAM
132 セキュアRAM領域
134 RAM領域
160₂
130 RAM型の記録媒体
KF₁, KF
CF
KF₁, KF
CF, KF₁
KF
105₂
SAM
メディア・ドライブSAM管理部
260
S165
操作部
S810
ホストCPU
165
810

【図４２】

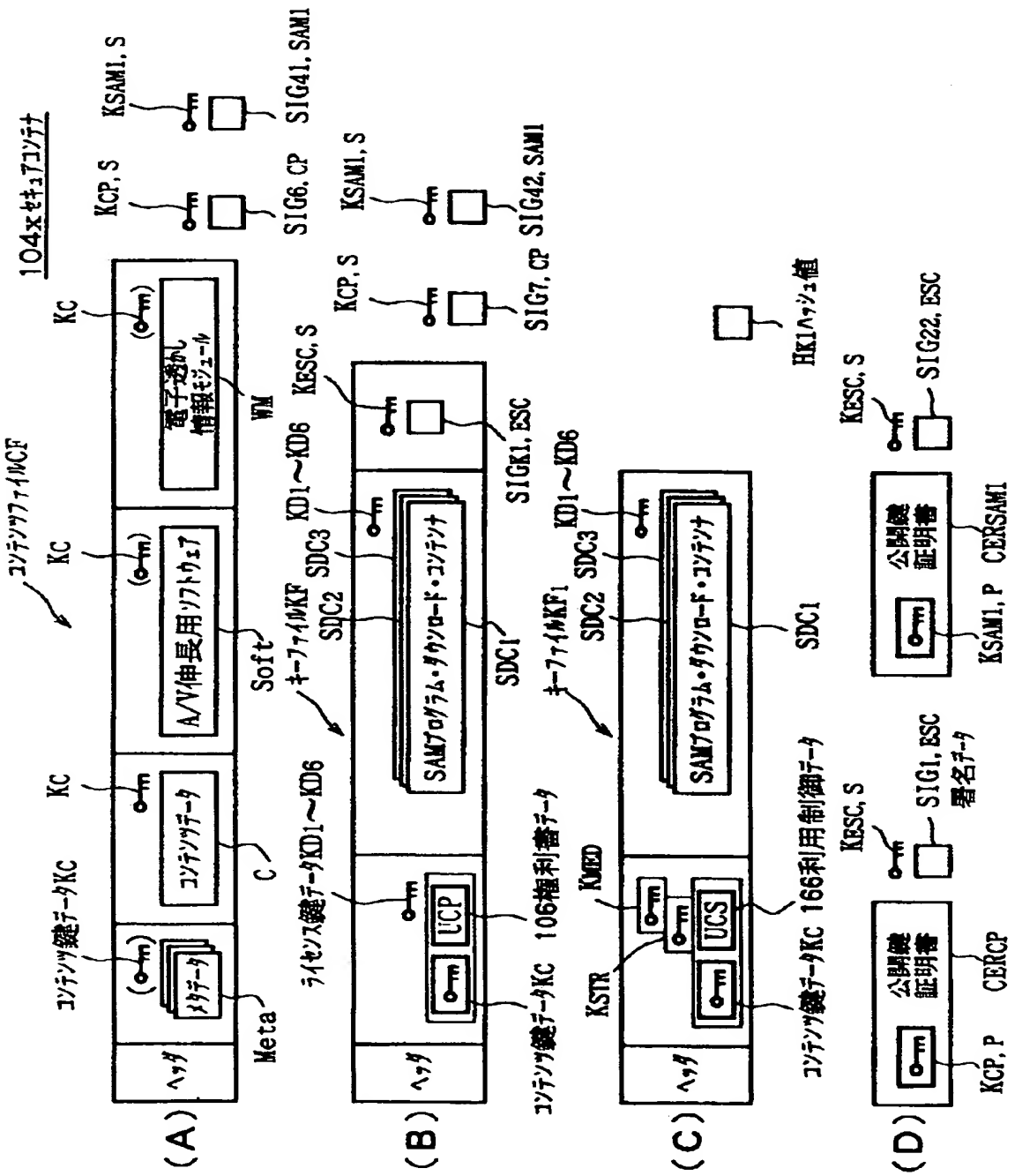

182
ダウンロードメモリ管理部
180
コンテンツプロバイダ管理部
184
AV圧縮・伸長用SAM管理部
185
EMDサービスセンタ管理部
104x
SAM管理部
190
メディアSAM管理部
197
作業要メモリ
200
外部メモリ管理部
811
105₁SAM
CF&SIG6, CP
KF&SIG7, CP
KF1&HK1
KF&SIG7, CP
KF1&HK1
166
186
利用監視部
暗号化・復号部
(KSESS)
171
暗号化・復号部
(KD1～KD3)
172
暗号化・復号部
(KSTR, KMMB, KPIM)
173
189
署名処理部
(KSAM1, S)
192
記憶部
187
課金処理部
CERSAM1, SIG22, ESC
CERCP, SIG1, ESC
KSESS
内部割り込み
S810
CPU
1100
相互認証部
170

【図４３】

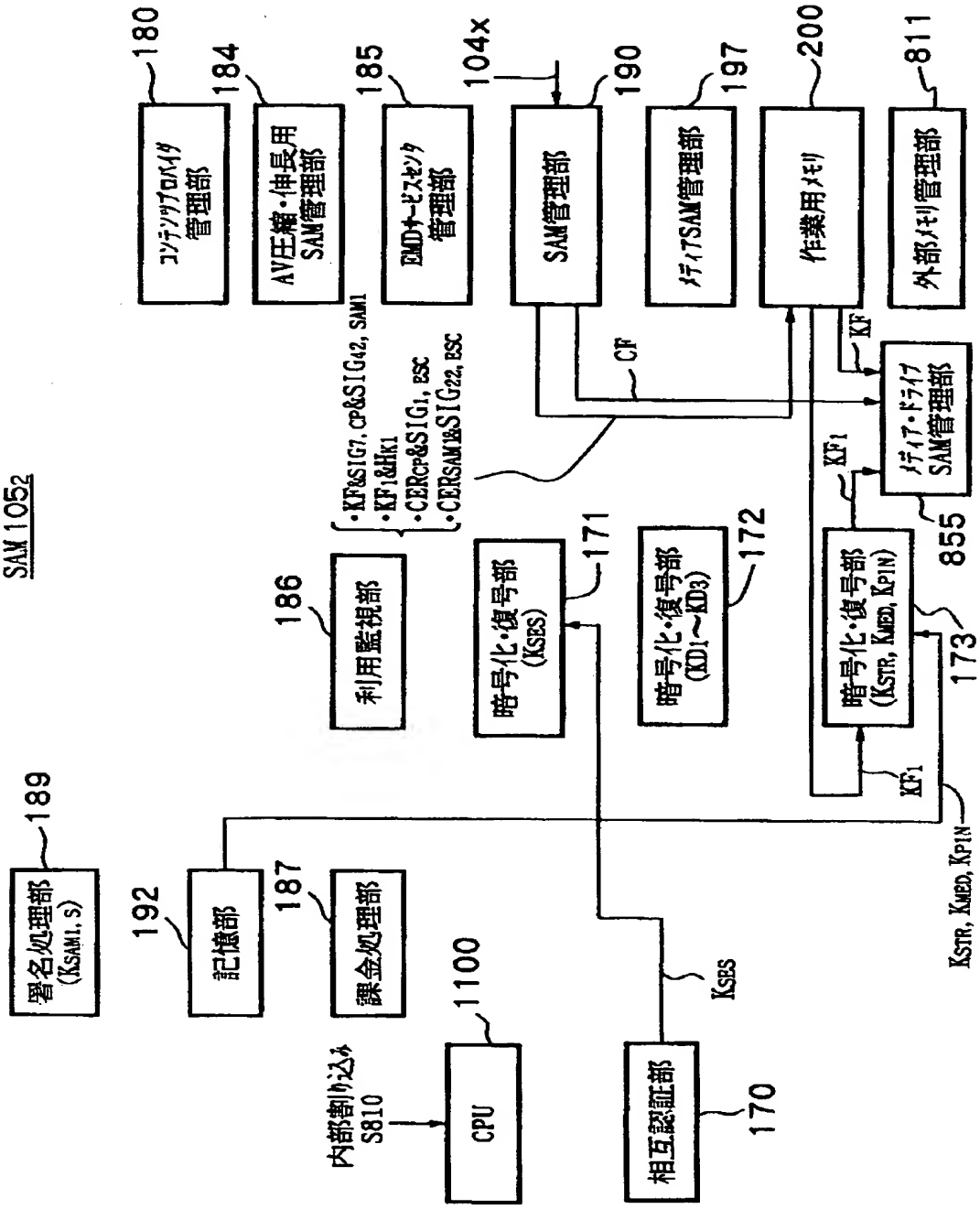
一の機器の利用制御データを使用して他の機器で再購入を行う場合の転送元のSAMの処理



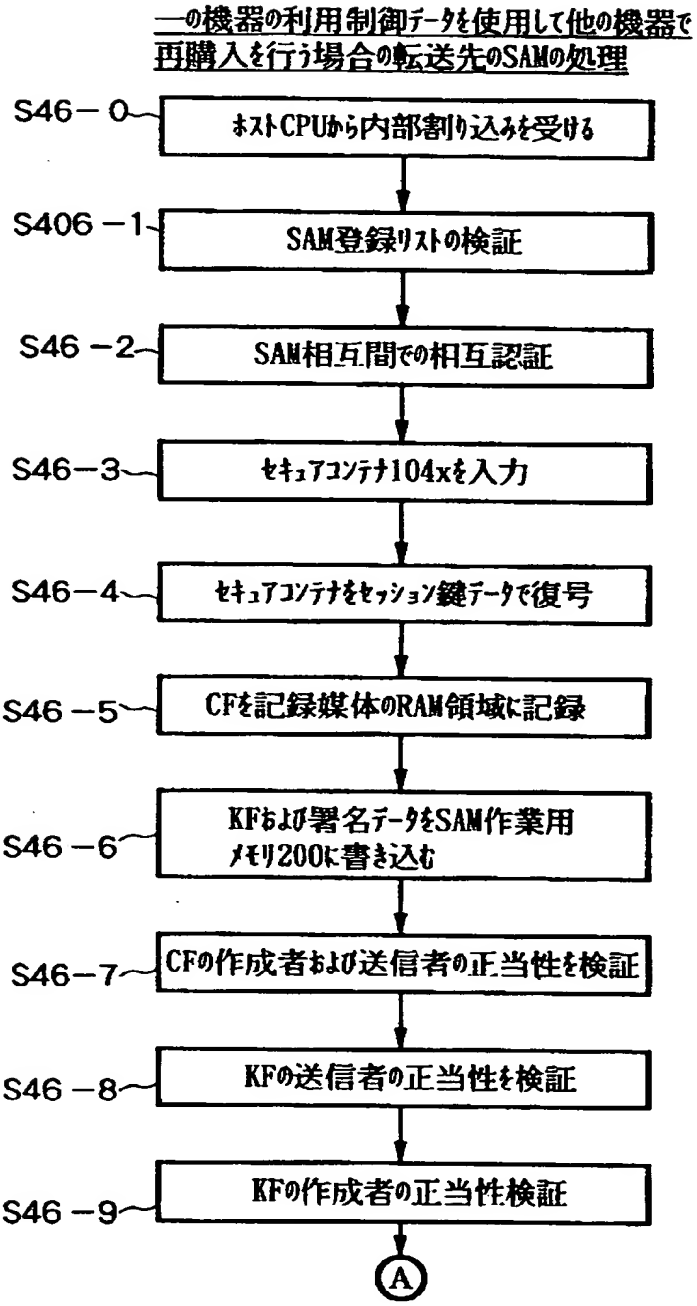
【図４４】


104xセキュアコンテナ
コンテンツファイルWCF
Kc
KCP, S
KSAM1, S
SIG41, SAM1
SIG6, CP
SIG42, SAM1
SIG7, CP
電子透かし情報モジュール
WM
A/V伸長用ソフトウェア
Soft
コンテンツデータ
C
メタデータ
Meta
コンテンツ鍵データKC
ライセンス鍵データKD1～KD6
キーファイルWKF
SDC2
SDC3
KD1～KD6
SAMプログラム・ダウンロード・コンテンツ
SDC1
KESC, S
SIGK1, ESC
UCP
コンテンツ鍵データKC
106権利書データ
キーファイルKF1
KMED
KSTR
UCS
166利用制御データ
HK1ハッシュ値
SIG22, ESC
公開鍵証明書
KSAM1, P
CERSAM1
SIG1, ESC
署名データ
KCP, P
CERCP
(A)
(B)
(C)
(D)

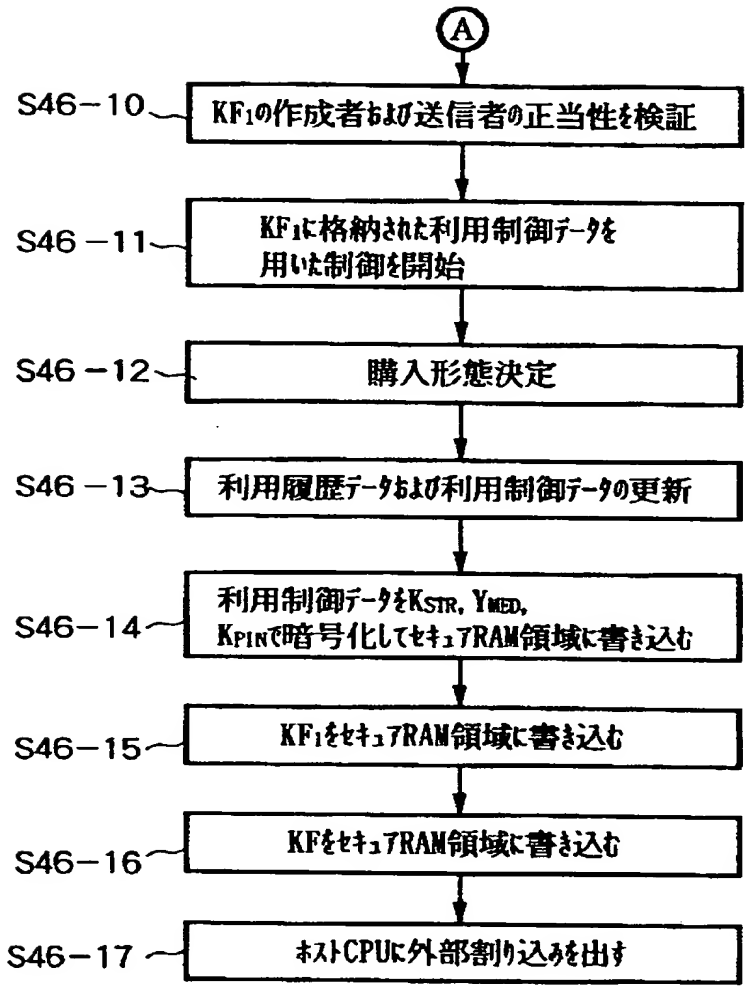
【図４５】


SAM 105₂
180
コンテンツプロバイダ管理部
184
AV圧縮・伸長用SAM管理部
185
EMDサービスセンタ管理部
104x
190
SAM管理部
197
メディアSAM管理部
200
作業用メモリ
811
外部メモリ管理部
・KF₀&SIG₇, CP&SIG₄₂, SAM₁
・KF₁&Hk₁
・CERCP&SIG₁, ESC
・CERSAM&SIG₂₂, ESC
CF
KF
KF₁
メディア・ドライブSAM管理部
855
186
利用監視部
暗号化・復号部(KSES)
171
暗号化・復号部(KD1～KD3)
172
暗号化・復号部(KSTR, KMED, KPIN)
173
189
署名処理部(KSAM1, S)
192
記憶部
187
課金処理部
1100
CPU
内部割り込み S810
相互認証部
170
KSES
KSTR, KMED, KPIN

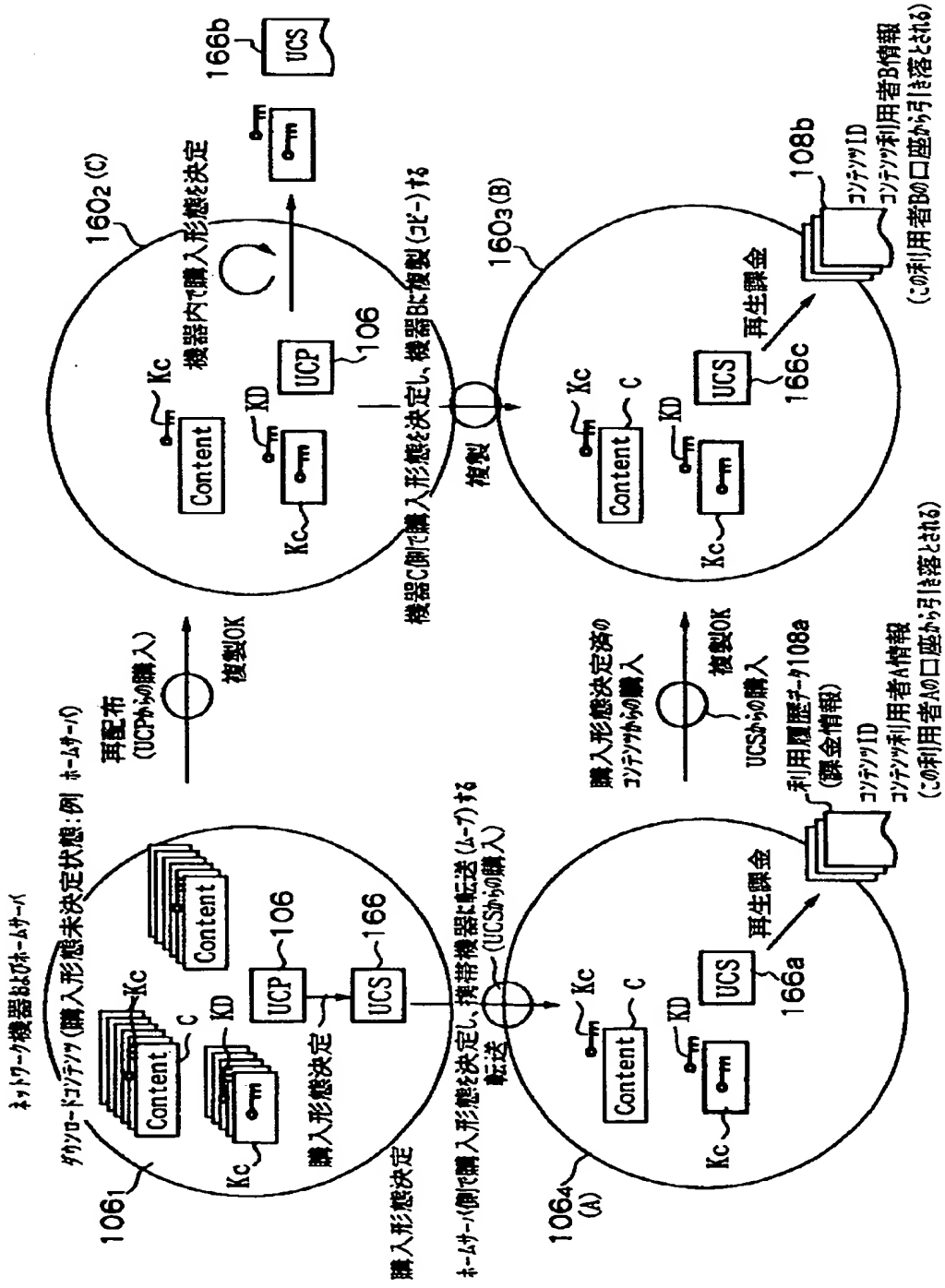
【図４６】


一の機器の利用制御データを使用して他の機器で再購入を行う場合の転送先のSAMの処理
S46－0
ホストCPUから内部割り込みを受ける
S406－1
SAM登録リストの検証
S46－2
SAM相互間での相互認証
S46－3
セキュアコンテナ104xを入力
S46－4
セキュアコンテナをセッション鍵データで復号
S46－5
CFを記録媒体のRAM領域に記録
S46－6
KFおよび署名データをSAM作業用メモリ200に書き込む
S46－7
CFの作成者および送信者の正当性を検証
S46－8
KFの送信者の正当性を検証
S46－9
KFの作成者の正当性検証
A

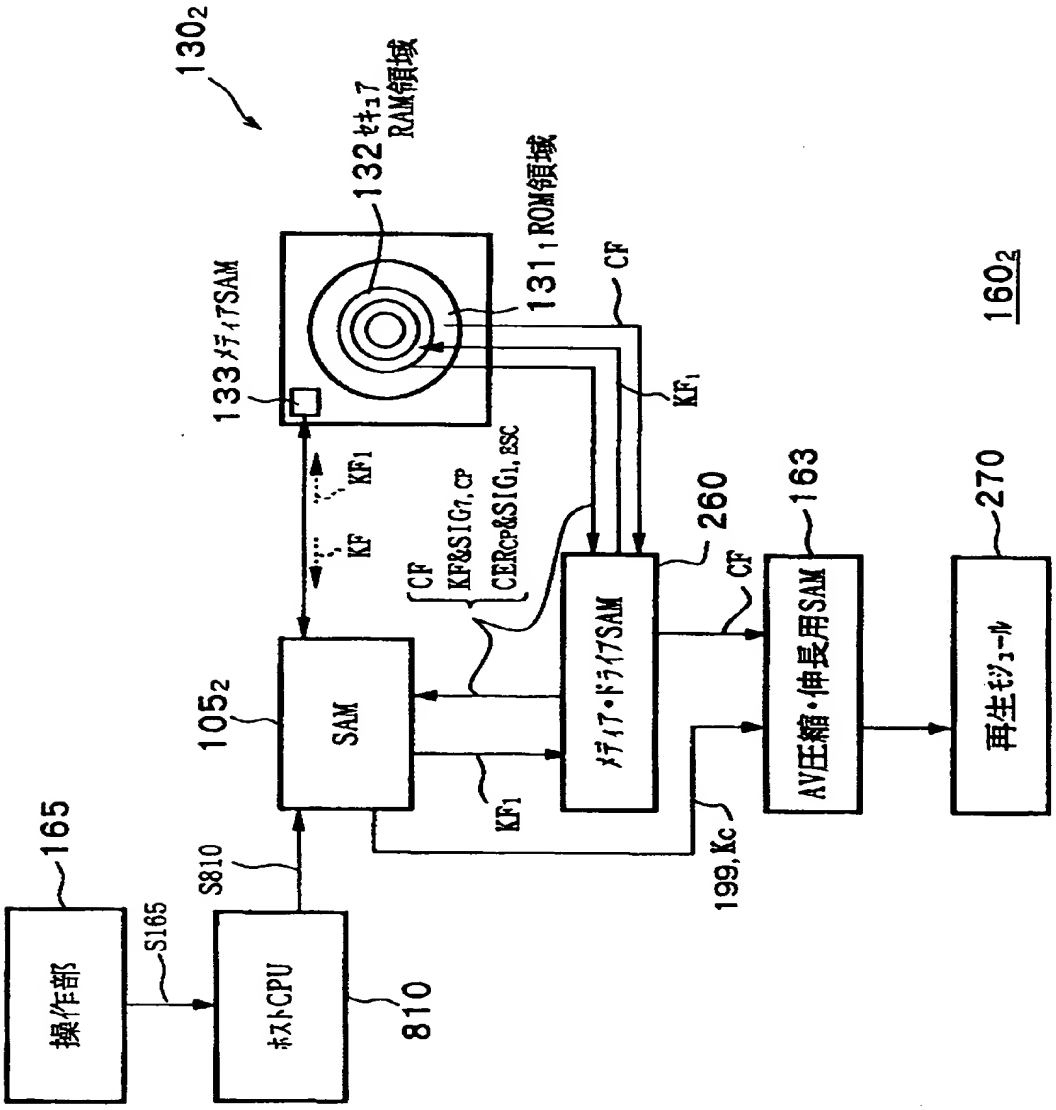
【図４７】


A
S46－10
KF1の作成者および送信者の正当性を検証
S46－11
KF1に格納された利用制御データを用いた制御を開始
S46－12
購入形態決定
S46－13
利用履歴データおよび利用制御データの更新
S46－14
利用制御データをKSTR, YMED, KPINで暗号化してセキュアRAM領域に書き込む
S46－15
KF1をセキュアRAM領域に書き込む
S46－16
KFをセキュアRAM領域に書き込む
S46－17
ホストCPUに外部割り込みを出す

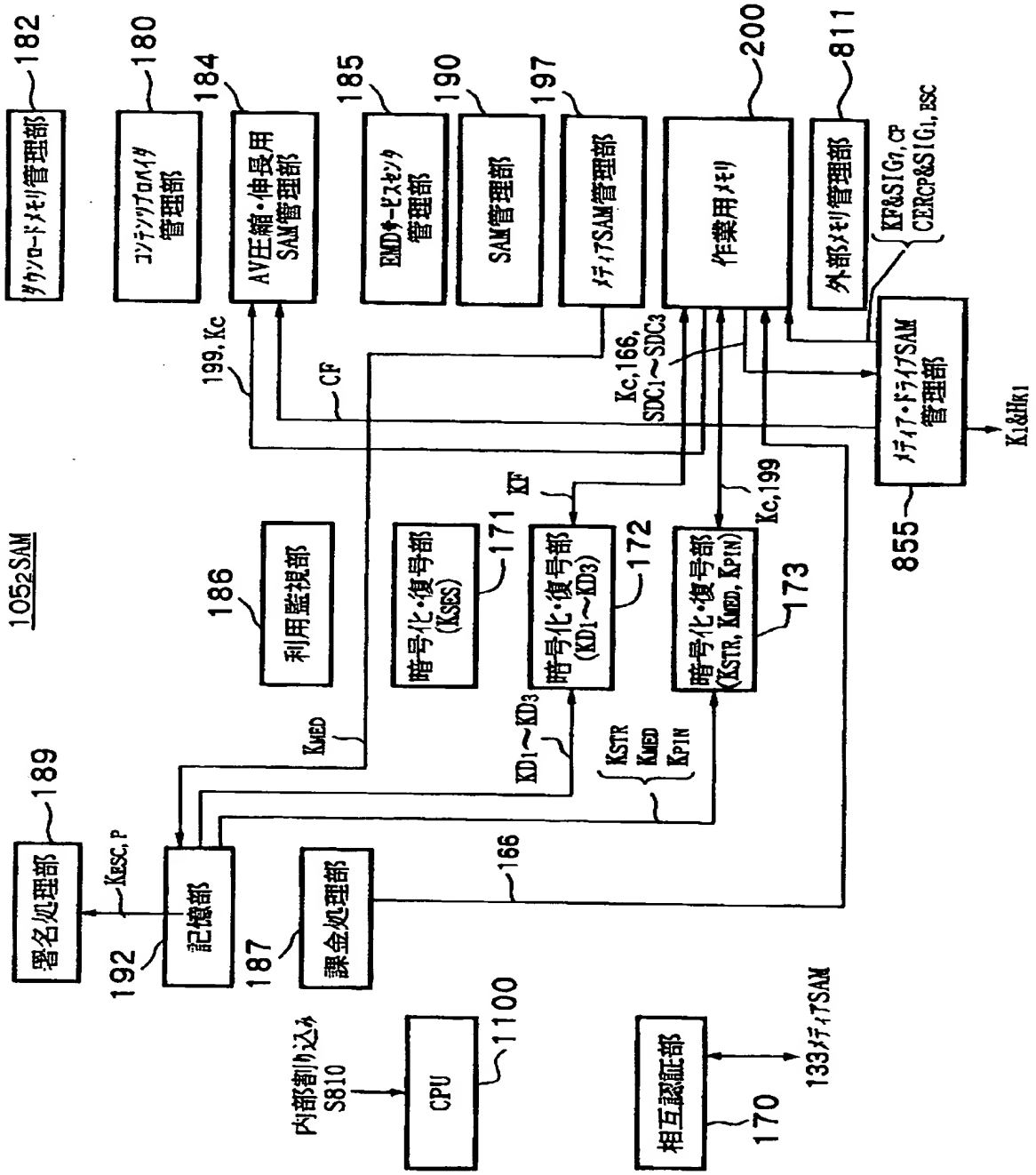
【図４８】


ネットワーク機器およびホームサーバ
ダウンロードコンテンツ（購入形態未決定状態：例 ホームサーバ）
Content
Kc
C
KD
UCP
106
UCS
166
購入形態決定
再配布
（UCPからの購入）
複製OK
1061
購入形態決定
ホームサーバ側で購入形態を決定し、携帯機器に転送（ムーブ）する
転送
（UCSからの購入）
1064
（A）
再生課金
利用履歴データ108a
（課金情報）
コンテンツID
コンテンツ利用者A情報
（この利用者Aの口座から引き落とされる）
購入形態決定済の
コンテンツからの購入
複製OK
UCSからの購入
166a
1602（C）
機器内で購入形態を決定
166b
機器C側で購入形態を決定し、機器Bに複製（コピー）する
複製
1603（B）
166c
108b
コンテンツID
コンテンツ利用者B情報
（この利用者Bの口座から引き落とされる）

【図４９】

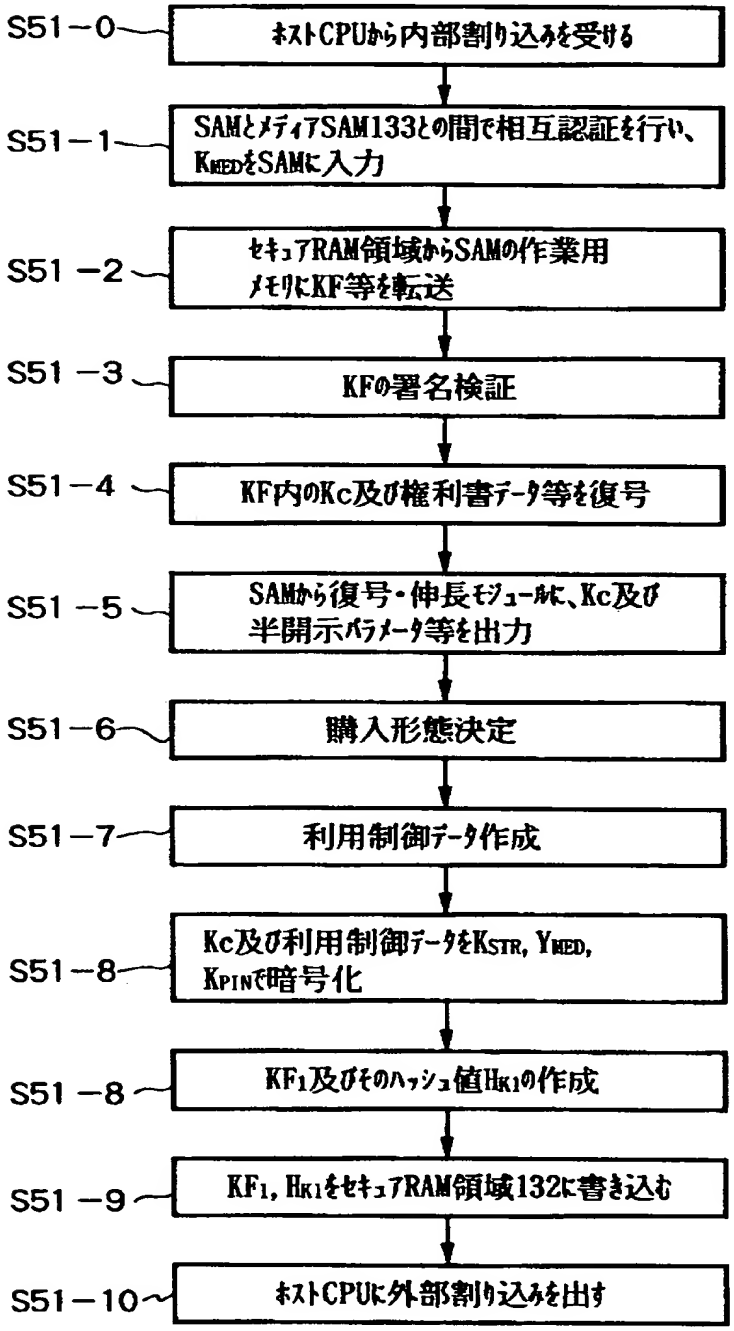

130_2
132 セキュリティRAM領域
131 ROM領域
133 メディアSAM
CF
KF_1
KF
KF_1
CF
KF&SIG1, CP
CERCP&SIG1, ESC
260
163
270
160_2
105_2
SAM
メディア・ドライブSAM
AV圧縮・伸長用SAM
再生モジュール
KF_1
199, Kc
165
S810
S165
操作部
ホストCPU
810

【図５０】

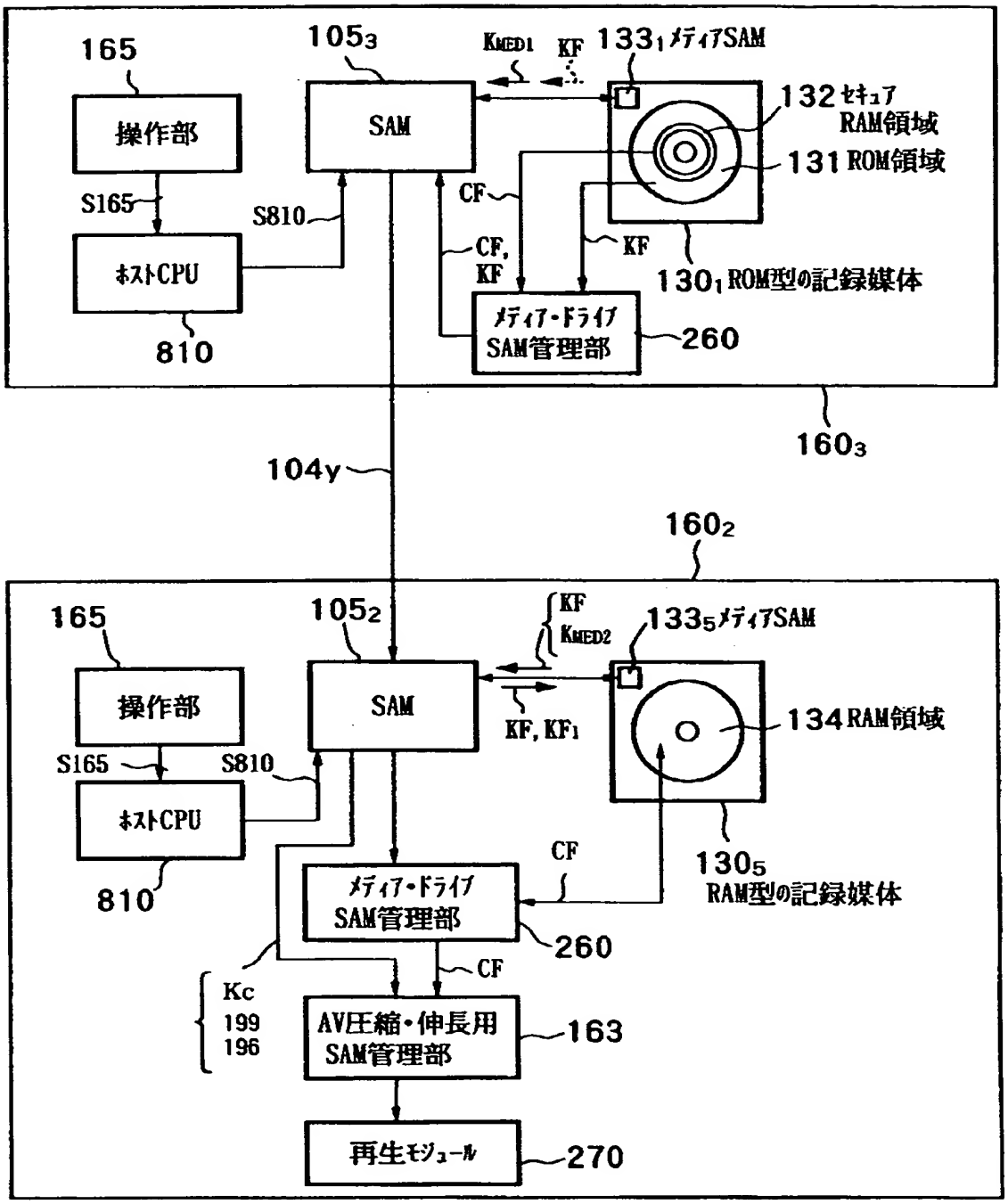

182
ダウンロードメモリ管理部
180
コンテンツプロバイダ管理部
184
AV圧縮・伸長用SAM管理部
185
EMDサービスセンタ管理部
190
SAM管理部
197
メディアSAM管理部
200
作業用メモリ
811
外部メモリ管理部
KF&SIG1, CP
CERCP&SIG1, ESC
199, Kc
CF
Kc,166,
SDC1～SDC3
メディア・ドライブSAM管理部
K1&HK1
855
105 2SAM
186
利用監視部
暗号化・復号部
(KSES)
171
KF
暗号化・復号部
(KD1～KD3)
172
Kc,199
暗号化・復号部
(KSTR, KMED, KPIN)
173
KMED
KD1～KD3
KSTR
KMED
KPIN
189
署名処理部
KESC, P
192
記憶部
187
課金処理部
166
内部割り込み
S810
CPU
1100
相互認証部
170
133メディアSAM

【図５１】

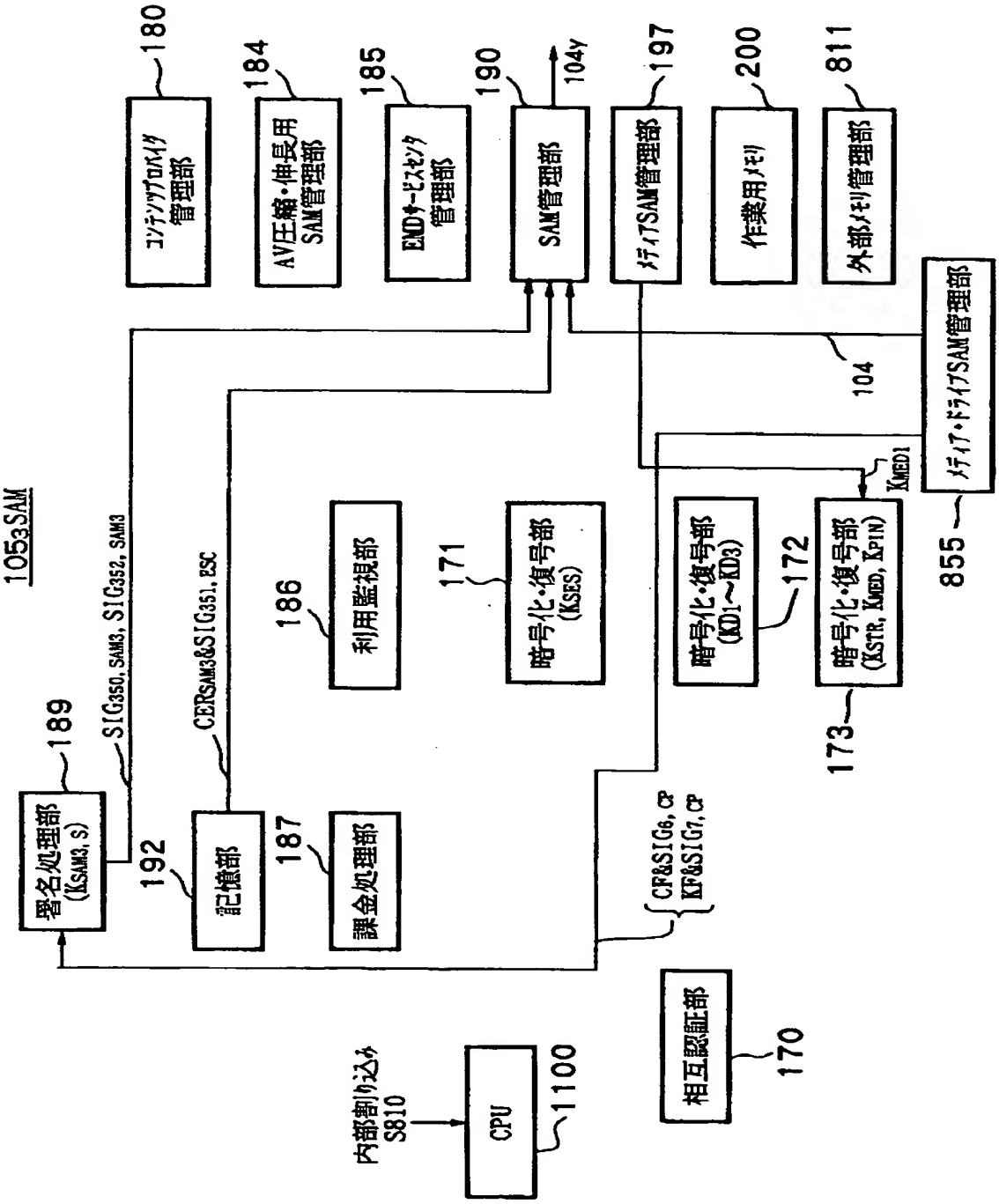
ROM型の記録媒体のコンテンツデータの購入形態決定処理



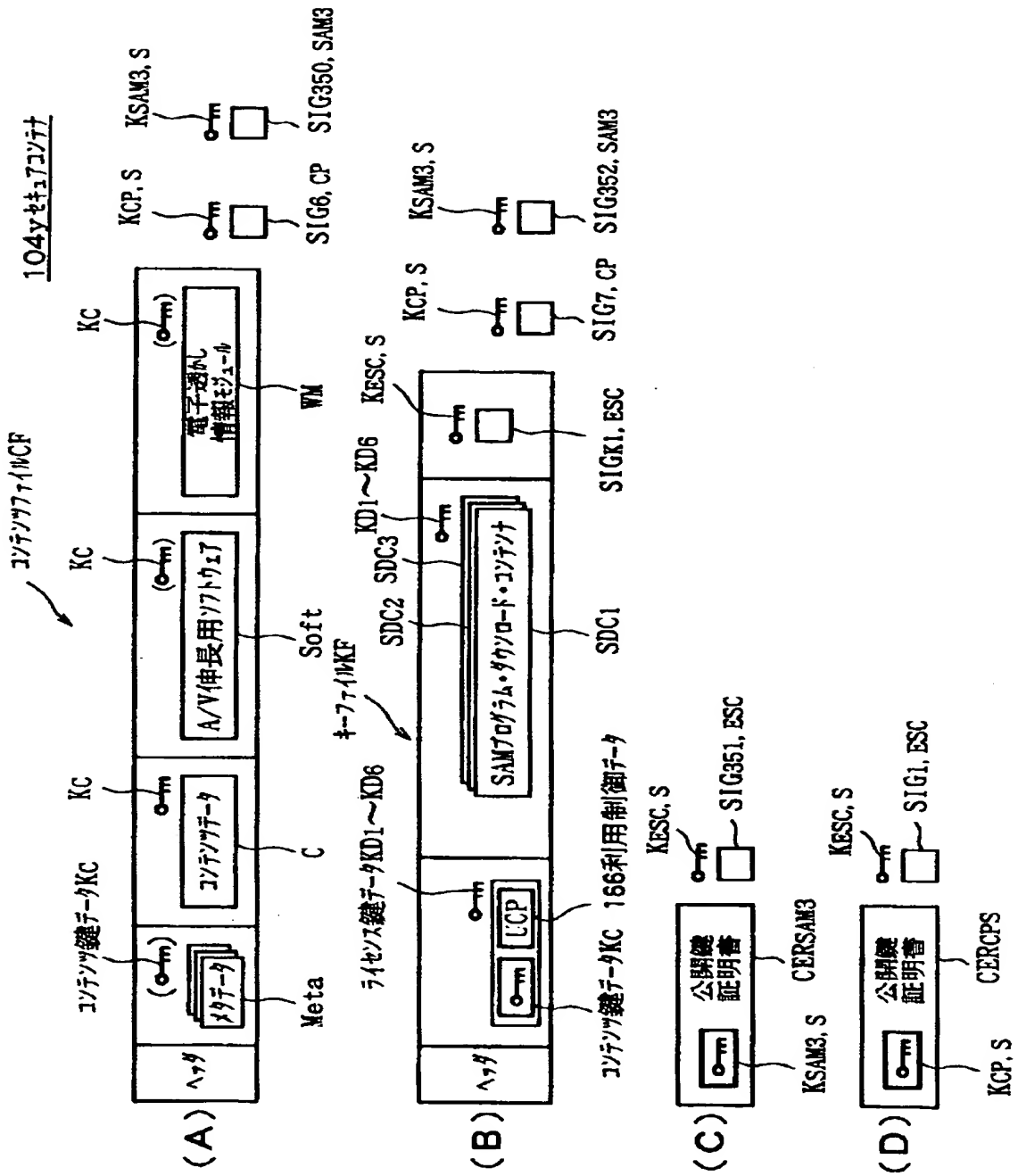
【図５２】


165
操作部
S165
ホストCPU
810
S810
105₃
SAM
KMED1
KF
133₁メディアSAM
132セキュアRAM領域
131 ROM領域
CF
CF, KF
KF
130₁ ROM型の記録媒体
メディア・ドライブ SAM管理部
260
160₃
104y
160₂
165
操作部
S165
ホストCPU
810
S810
105₂
SAM
KF
KMED2
133₅メディアSAM
KF, KF₁
134 RAM領域
130₅ RAM型の記録媒体
CF
メディア・ドライブ SAM管理部
260
CF
Kc
199
196
AV圧縮・伸長用 SAM管理部
163
再生モジュール
270

【図５３】

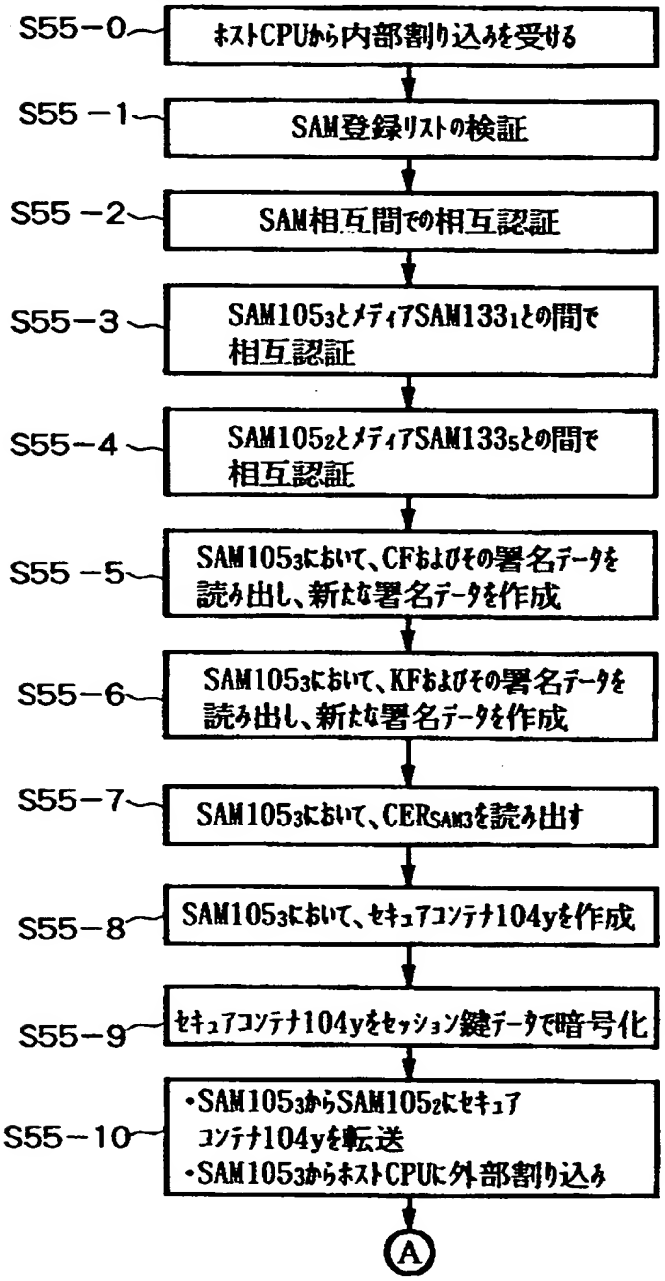

105₃SAM
189
署名処理部 (KSAM3, S)
192
記憶部
187
課金処理部
186
利用監視部
171
暗号化・復号部 (KSES)
暗号化・復号部 (KD1～KD3)
172
暗号化・復号部 (KSTR, KMED, KPIN)
173
855
メディア・ドライブSAM管理部
KMED1
104
メディアSAM管理部
197
作業用メモリ
200
外部メモリ管理部
811
SAM管理部
190
104y
END-ユーザセンタ管理部
185
AV圧縮・伸長用SAM管理部
184
コンテンツプロバイダ管理部
180
SIG350, SAM3, SIG352, SAM3
CERSAM3&SIG351, ESC
CR&SIG6, CP
KF&SIG7, CP
相互認証部
170
CPU
1100
内部割り込み S810

【図５４】

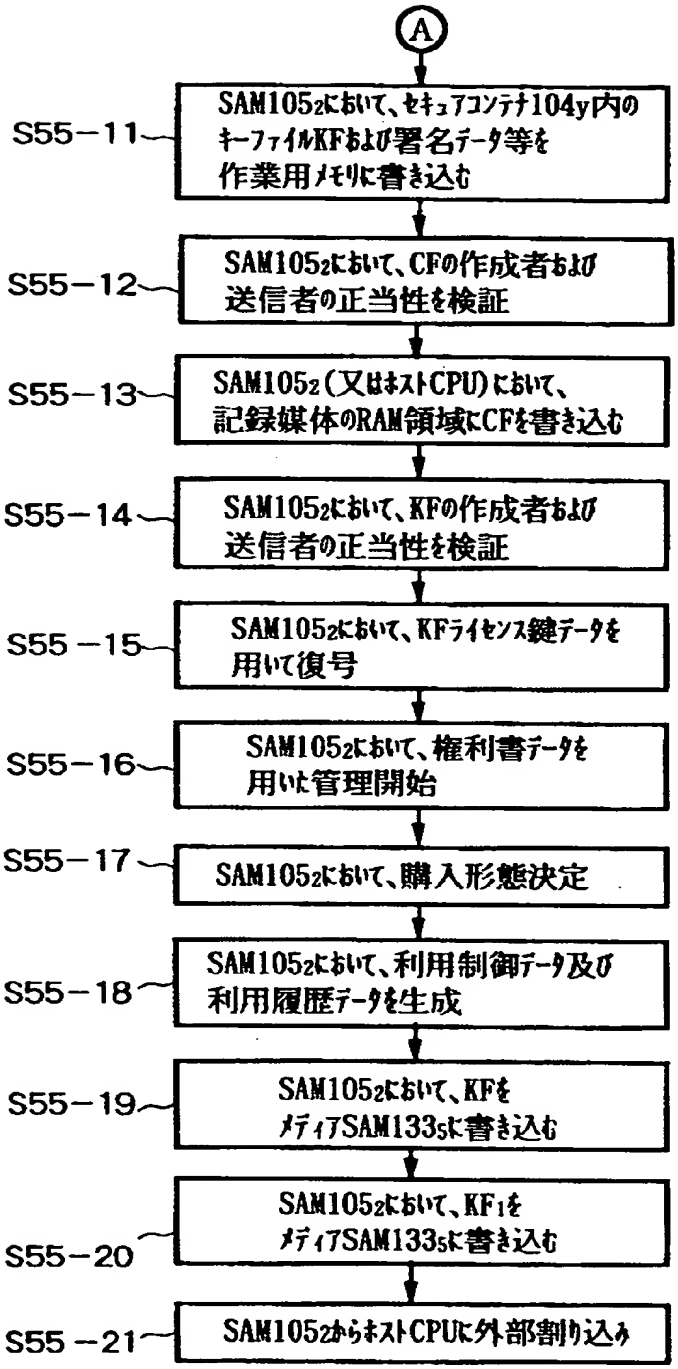

104ｙセキュリティ
KSAM3, S
SIG350, SAM3
KCP, S
SIG6, CP
KC
コンテンツファイルCF
電子透かし情報モジュール
WM
A/V伸長用ソフトウェア
Soft
コンテンツデータ
C
メタデータ
Meta
コンテンツ鍵データKc
KC
ヘッダ
(A)
KSAM3, S
SIG352, SAM3
KCP, S
SIG7, CP
KESC, S
SIGK1, ESC
KD1～KD6
SDC3
SDC2
SDC1
SAMプログラム・ダウンロード・コンテンツ
キーファイルKF
ライセンス鍵データKD1～KD6
LCP
コンテンツ鍵データKc
166利用制御データ
ヘッダ
(B)
KESC, S
SIG351, ESC
公開鍵証明書
CERSAM3
KSAM3, S
(C)
KESC, S
SIG1, ESC
公開鍵証明書
CERCPS
KCP, S
(D)

【図５５】

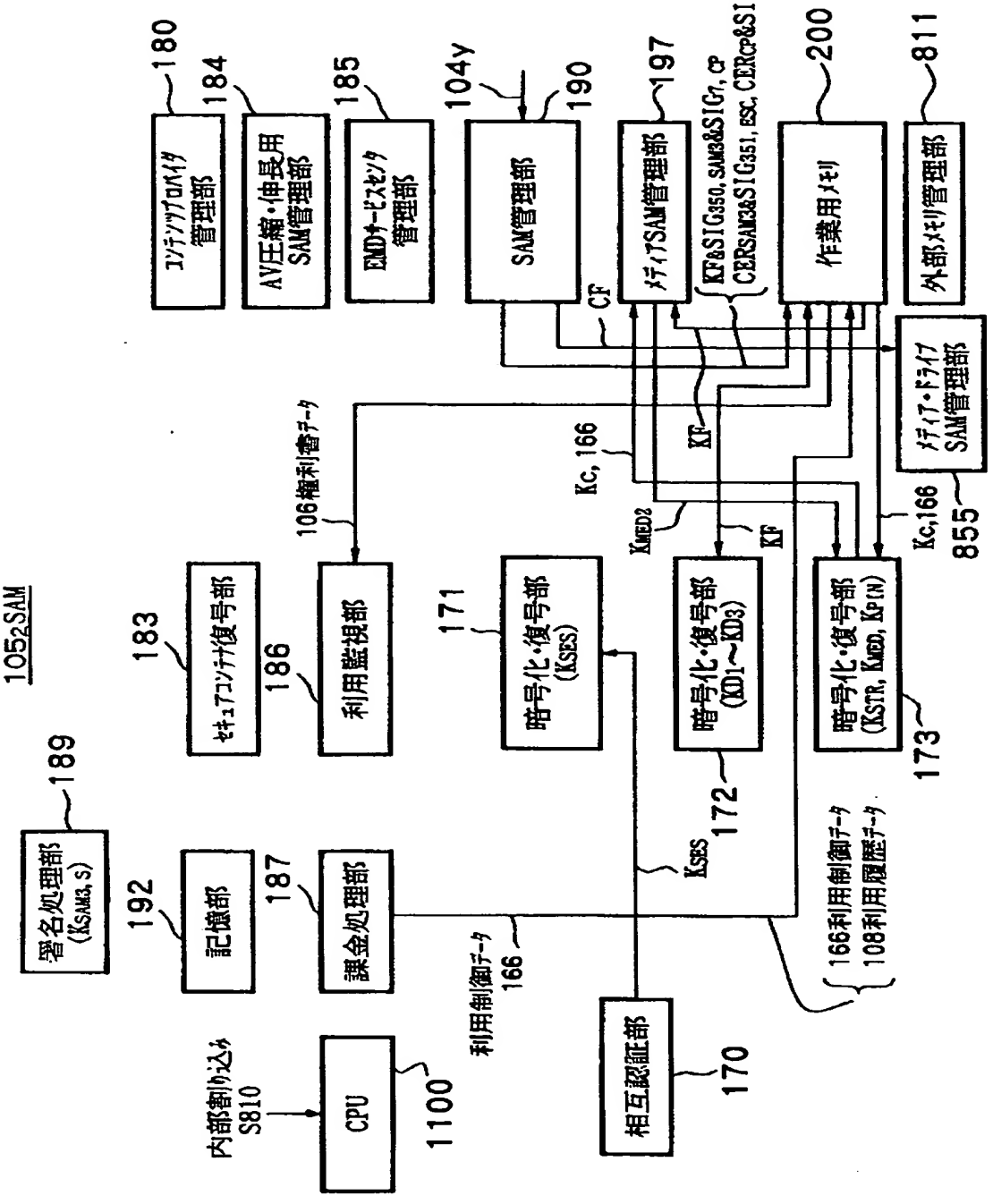
ROM型の記録媒体のコンテンツデータを転送した後に転送先で
購入形態を決定してRAM型の記録媒体に書き込む場合の処理



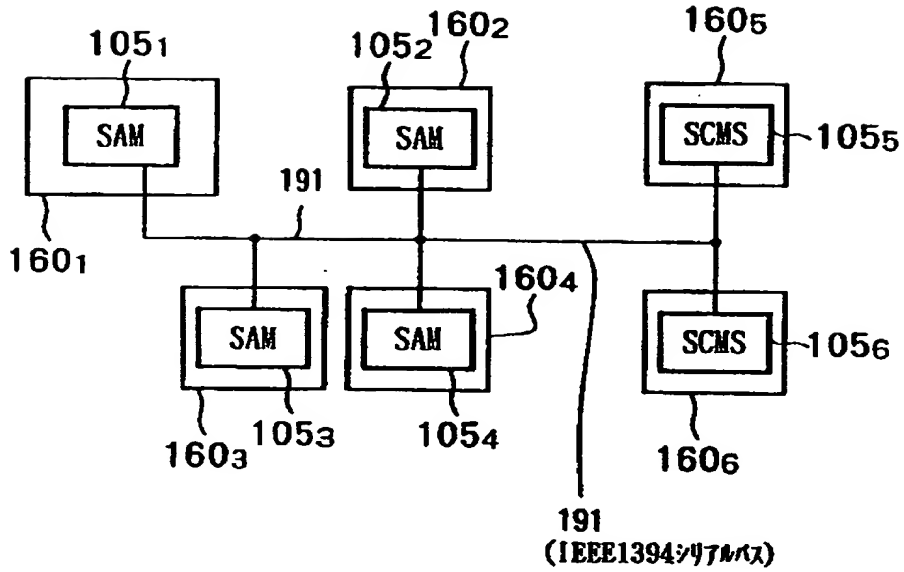
【図５６】


A
S55－11
SAM105₂において、セキュアコンテナ104y内のキーファイルKFおよび署名データ等を作業用メモリに書き込む
S55－12
SAM105₂において、CFの作成者および送信者の正当性を検証
S55－13
SAM105₂（又はホストCPU）において、記録媒体のRAM領域にCFを書き込む
S55－14
SAM105₂において、KFの作成者および送信者の正当性を検証
S55－15
SAM105₂において、KFライセンス鍵データを用いて復号
S55－16
SAM105₂において、権利書データを用いた管理開始
S55－17
SAM105₂において、購入形態決定
S55－18
SAM105₂において、利用制御データ及び利用履歴データを生成
S55－19
SAM105₂において、KFをメディアSAM133₅に書き込む
S55－20
SAM105₂において、KF₁をメディアSAM133₅に書き込む
S55－21
SAM105₂からホストCPUに外部割り込み

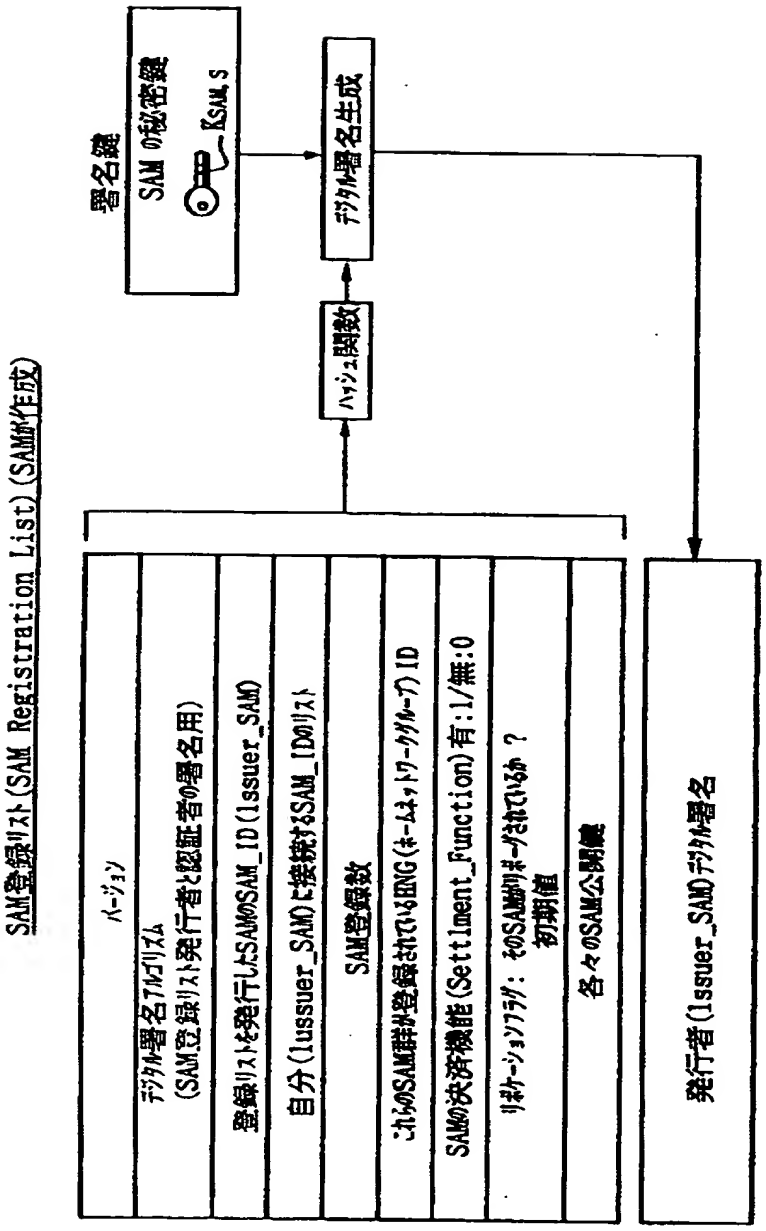
【図５７】


105₂SAM
署名処理部 (KSAM3, S)
189
記憶部
192
課金処理部
187
CPU
1100
内部割り込み S810
利用制御データ 166
セキュアコンテナ復号部
183
186
利用監視部
106権利書データ
171
暗号化・復号部 (KSES)
KSES
暗号化・復号部 (KD1～KD3)
172
暗号化・復号部 (KSTR, KMED, KP(N))
173
166利用制御データ
108利用履歴データ
相互認証部
170
Kc, 166
KMED2
KF
KF&SIG350, SAM3&SIG1, CP
CERSAM3&SIG351, ESC, CERCP&SIG1, ESC
CF
メディアSAM管理部
197
メディア・ドライブ SAM管理部
855
Kc,166
コンテンツプロバイダ 管理部
180
AV圧縮・伸長用 SAM管理部
184
EMDサービスセンタ 管理部
185
SAM管理部
104y
190
作業用メモリ
200
外部メモリ管理部
811

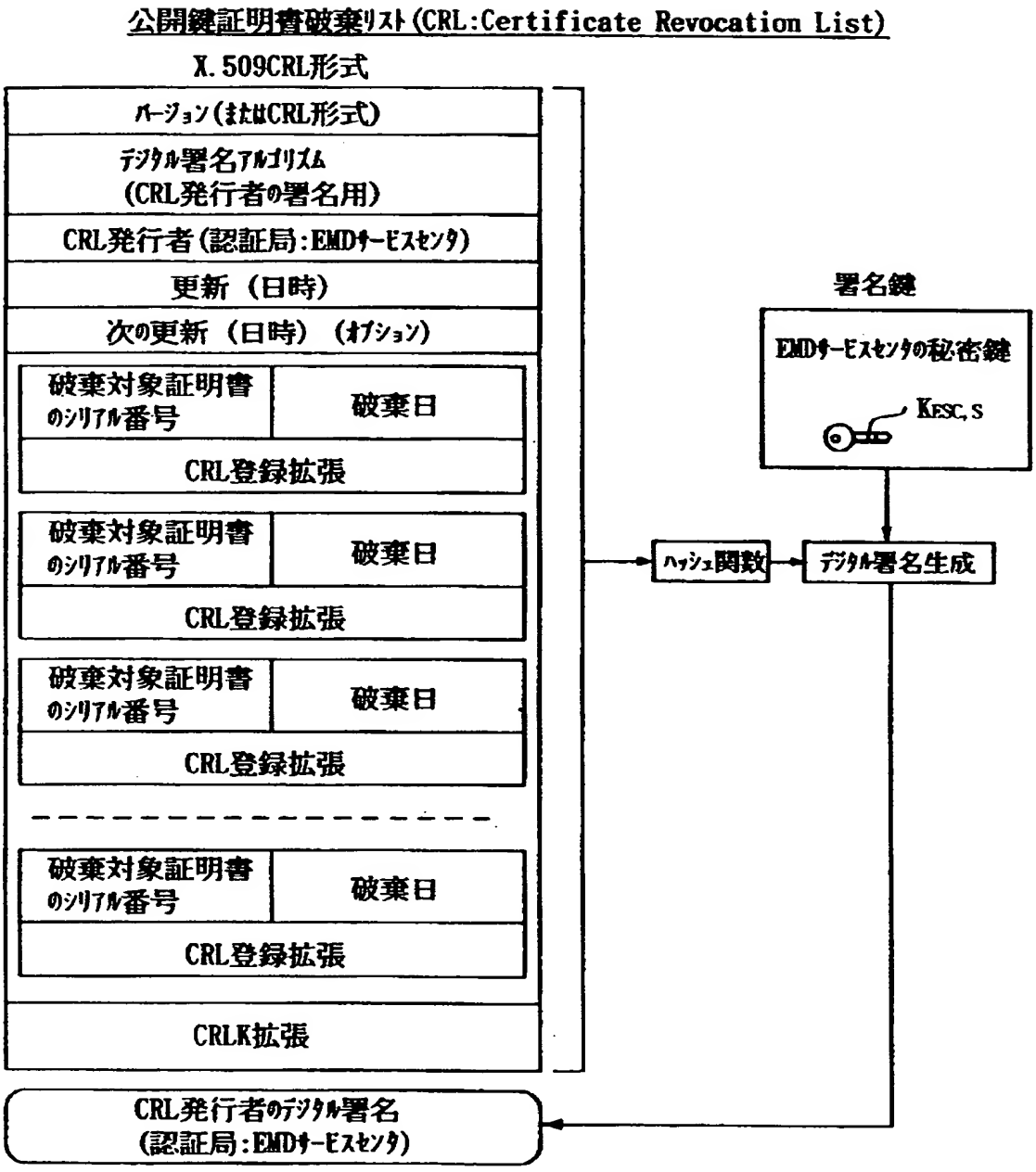
【図５８】


1051
1052
1602
1605
SAM
SAM
SCMS
1055
191
1601
1604
SAM
SAM
SCMS
1056
1603
1053
1054
1606
191
(IEEE1394シリアルバス)

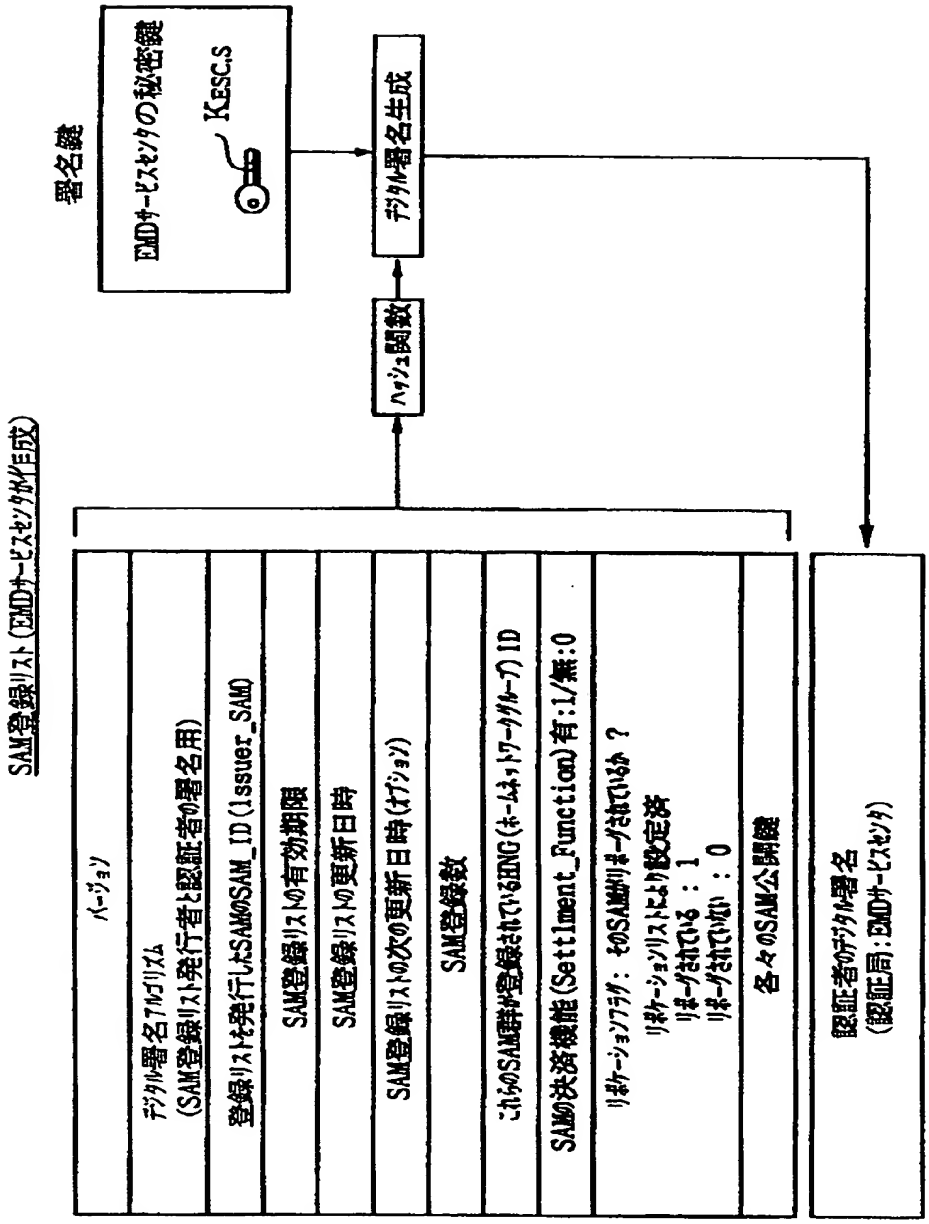
【図５９】


SAM登録リスト(SAM Registration List)(SAM作成)
バージョン
デジタル署名アルゴリズム
(SAM登録リスト発行者と認証者の署名用)
登録リストを発行したSAMのSAM_ID(Issuer_SAM)
自分(Issuer_SAM)に接続するSAM_IDのリスト
SAM登録数
これらのSAM群が登録されているBNG(ホームネットワークグループ)ID
SAMの決済機能(Settlment_Function)有:1/無:0
リボルバージョンフラグ: そのSAMのリボークされているか？
初期値
各々のSAM公開鍵
発行者(Issuer_SAM)デジタル署名
ハッシュ関数
デジタル署名生成
署名鍵
SAM の秘密鍵
KSAM,S

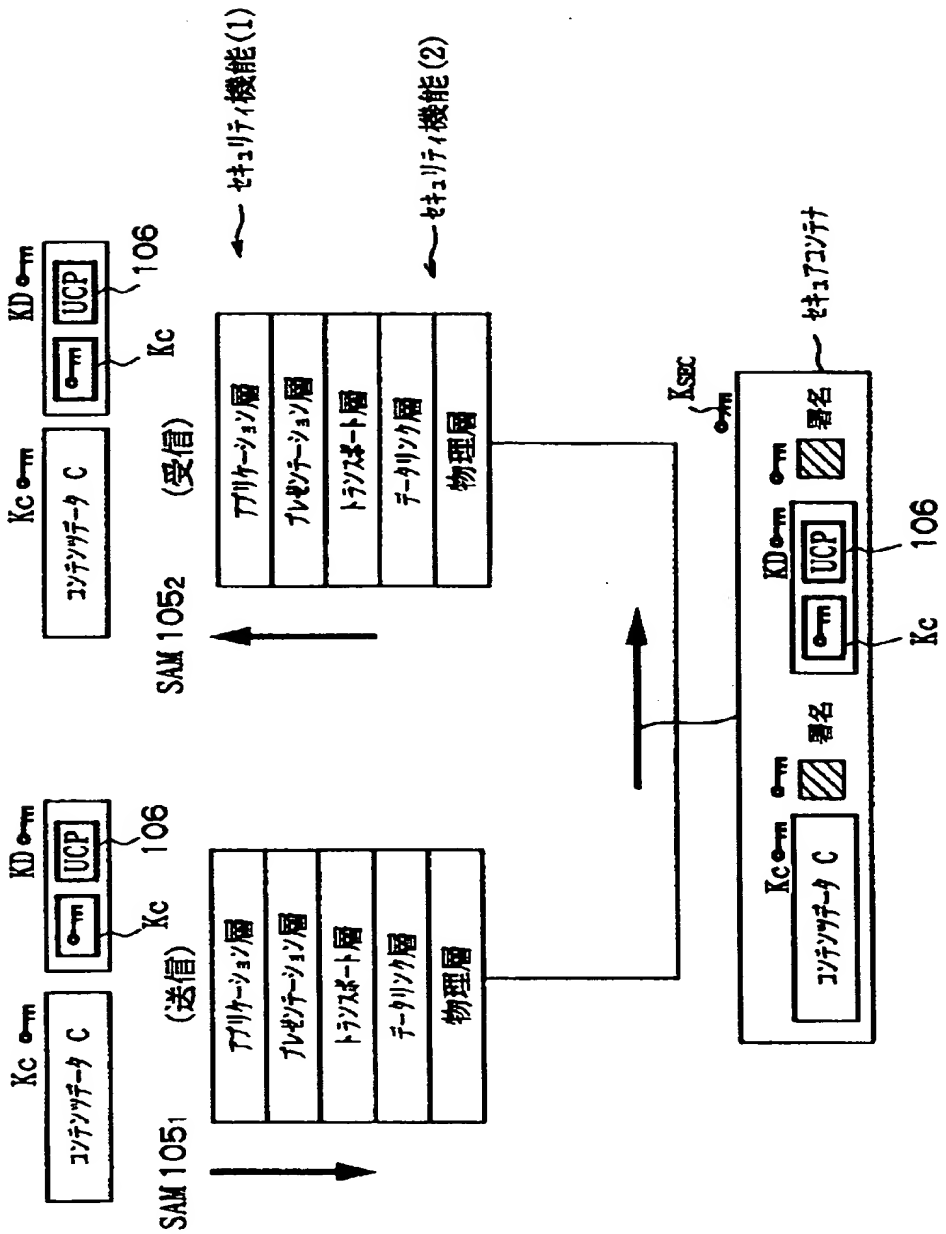
【図６０】


公開鍵証明書破棄リスト(CRL:Certificate Revocation List)
X.509CRL形式
バージョン(またはCRL形式)
デジタル署名アルゴリズム
(CRL発行者の署名用)
CRL発行者(認証局:EMDサービスセンタ)
更新（日時）
次の更新（日時）（オプション）
破棄対象証明書のシリアル番号
破棄日
CRL登録拡張
破棄対象証明書のシリアル番号
破棄日
CRL登録拡張
破棄対象証明書のシリアル番号
破棄日
CRL登録拡張
破棄対象証明書のシリアル番号
破棄日
CRL登録拡張
CRLK拡張
CRL発行者のデジタル署名
(認証局:EMDサービスセンタ)
署名鍵
EMDサービスセンタの秘密鍵
KESC,S
ハッシュ関数
デジタル署名生成

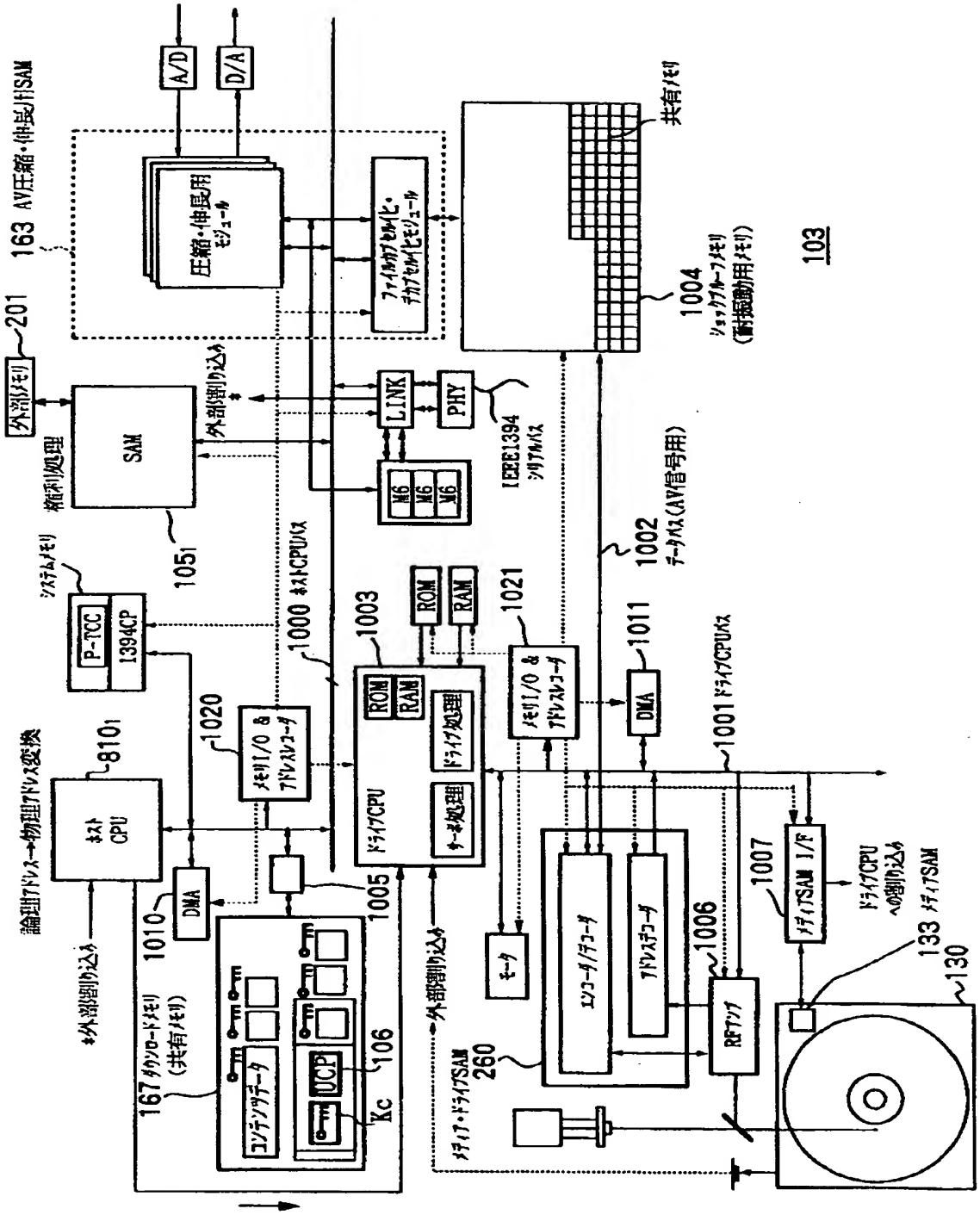
【図６１】


署名鍵
EMDサービスセンタの秘密鍵
KESCS
ハッシュ関数
デジタル署名生成
SAM登録リスト（EMDサービスセンタが作成）
バージョン
デジタル署名アルゴリズム
（SAM登録リスト発行者と認証者の署名用）
登録リストを発行したSAMのSAM_ID（Issuer_SAM）
SAM登録リストの有効期限
SAM登録リストの更新日時
SAM登録リストの次の更新日時（オプション）
SAM登録数
これらのSAM群が登録されているRNG（ホームネットワークグループ）ID
SAMの決済機能（Settlment_Function）有：1/無：0
リボケーションフラグ：そのSAMがリボークされているか？
リボケーションリストにより設定済
リボークされている：1
リボークされていない：0
各々のSAM公開鍵
認証者のデジタル署名
（認証局：EMDサービスセンタ）

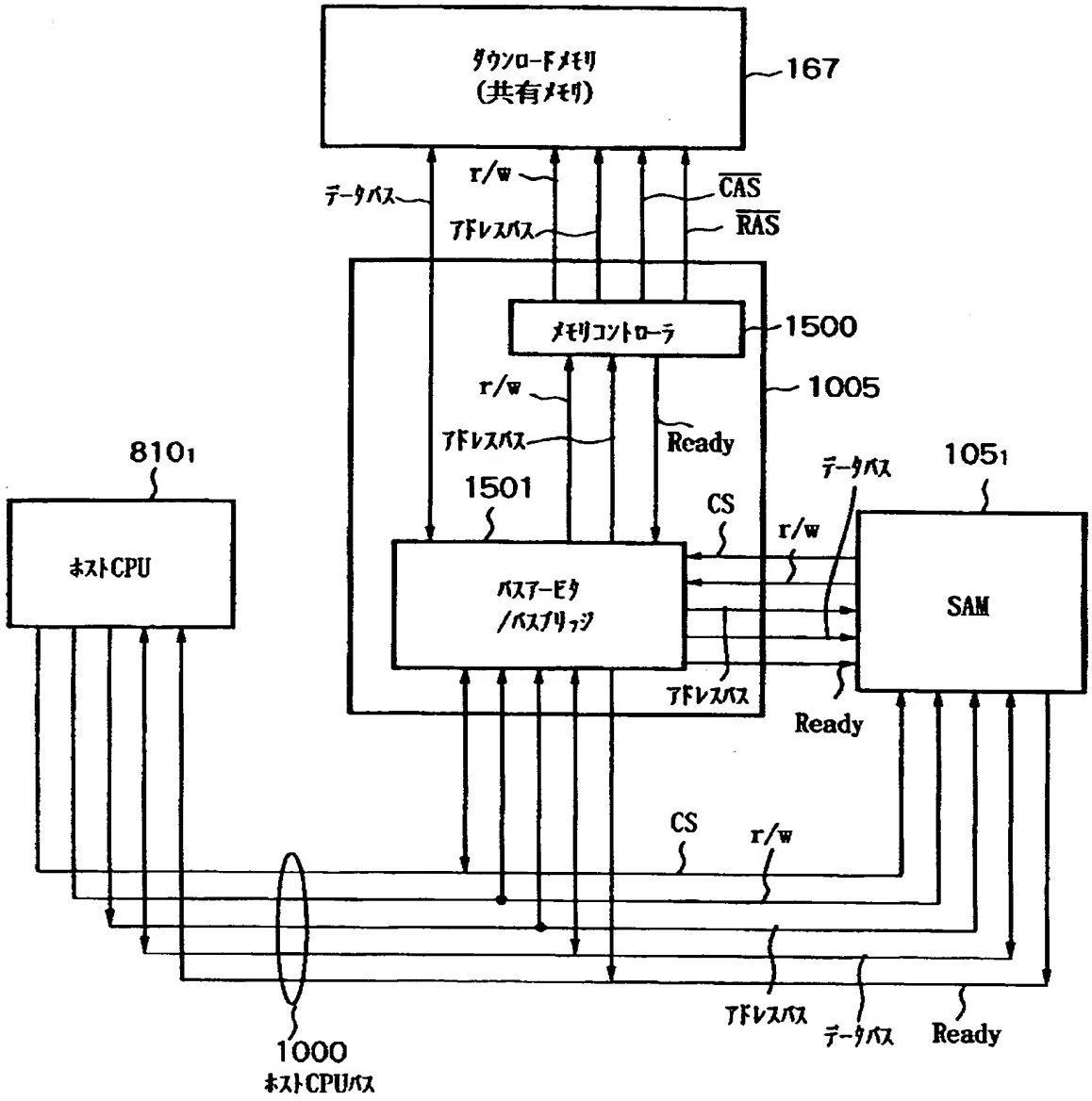
【図６２】


セキュリティ機能(1)
セキュリティ機能(2)
セキュアコンテナ
KD
UCP
106
Kc
Ksec
コンテンツデータ C
署名
アプリケーション層
プレゼンテーション層
トランスポート層
データリンク層
物理層
SAM 105₂
(受信)
SAM 105₁
(送信)

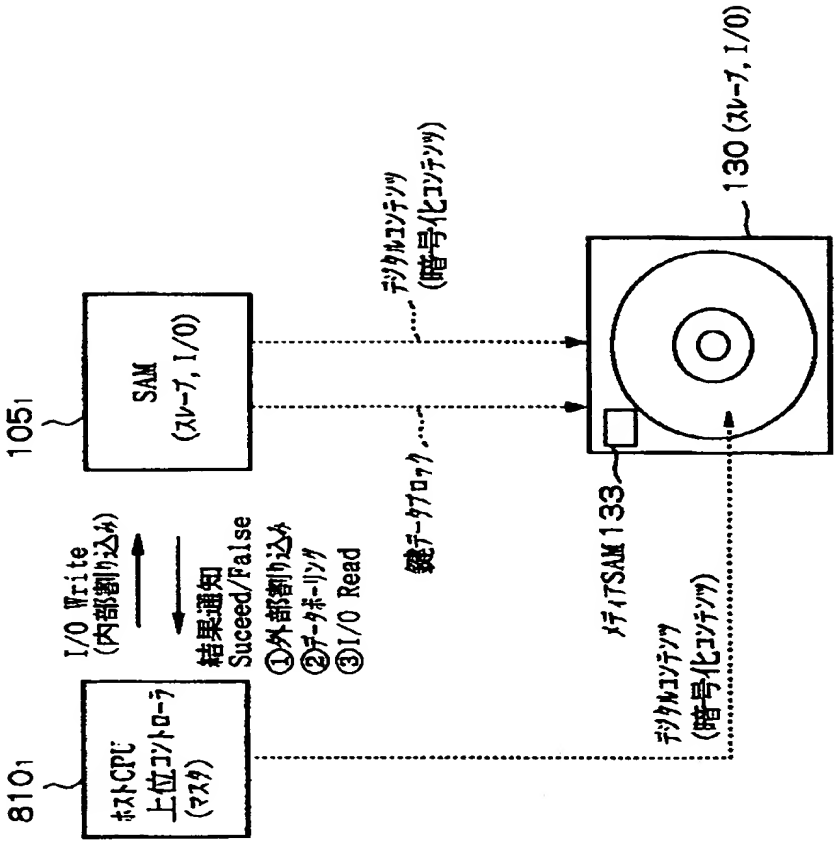
【図６３】


A/D
D/A
163 AV圧縮・伸長用SAM
圧縮・伸長用モジュール
ファイルカプセル化・デカプセル化モジュール
共有メモリ
1004
ショックプルーフメモリ（耐振動用メモリ）
103
201
外部メモリ
SAM
外部割込み
L-LINK
PHY
IEEE1394シリアルバス
M6
M6
M6
1051
システムメモリ
P-TCC
1394CP
1000 ホストCPUバス
1003
ROM
RAM
1021
1002 データバス（AV信号用）
1020
メモリI/O & アドレスデコーダ
ドライブ処理
ホスト処理
ドライブCPU
1011
DMA
1001 ドライブCPUバス
論理アドレス→物理アドレス変換
ホストCPU
8101
DMA
1010
1005
外部割込み
ホスト外部割込み
167 ダウンロードメモリ（共有メモリ）
コンテンツデータ
UCP
Kc
106
ドライブSAM
260
モータ
エンコーダ/デコーダ
アドレスデコーダ
1006
RFアンプ
1007
メディアSAM I/F
ドライブCPUへの割込み
133 メディアSAM
130

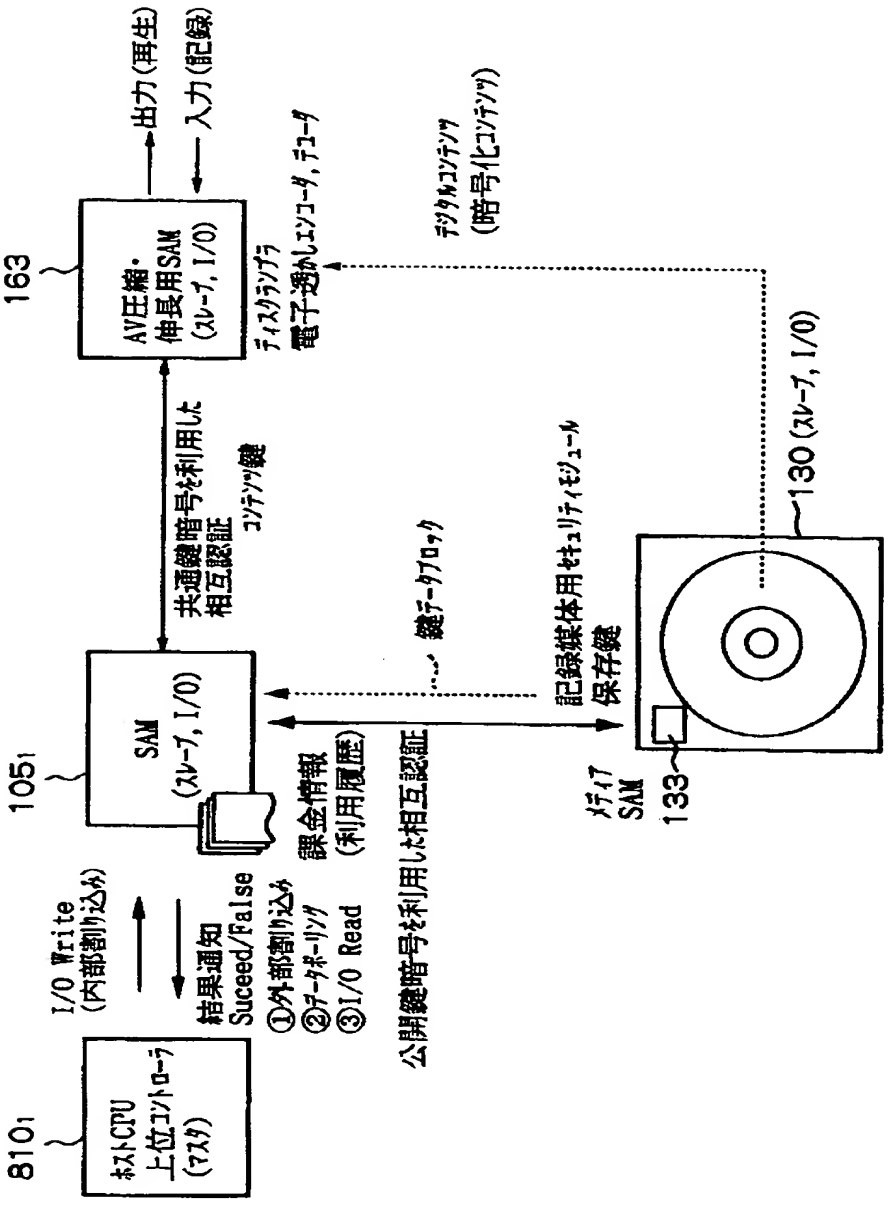
【図６４】


ダウンロードメモリ
(共有メモリ)
167
データバス
r/w
アドレスバス
CAS
RAS
メモリコントローラ
1500
1005
r/w
アドレスバス
Ready
1501
CS
r/w
データバス
SAM
1051
ホストCPU
8101
バスアービタ
/バスブリッジ
アドレスバス
Ready
CS
r/w
アドレスバス
データバス
Ready
1000
ホストCPUバス

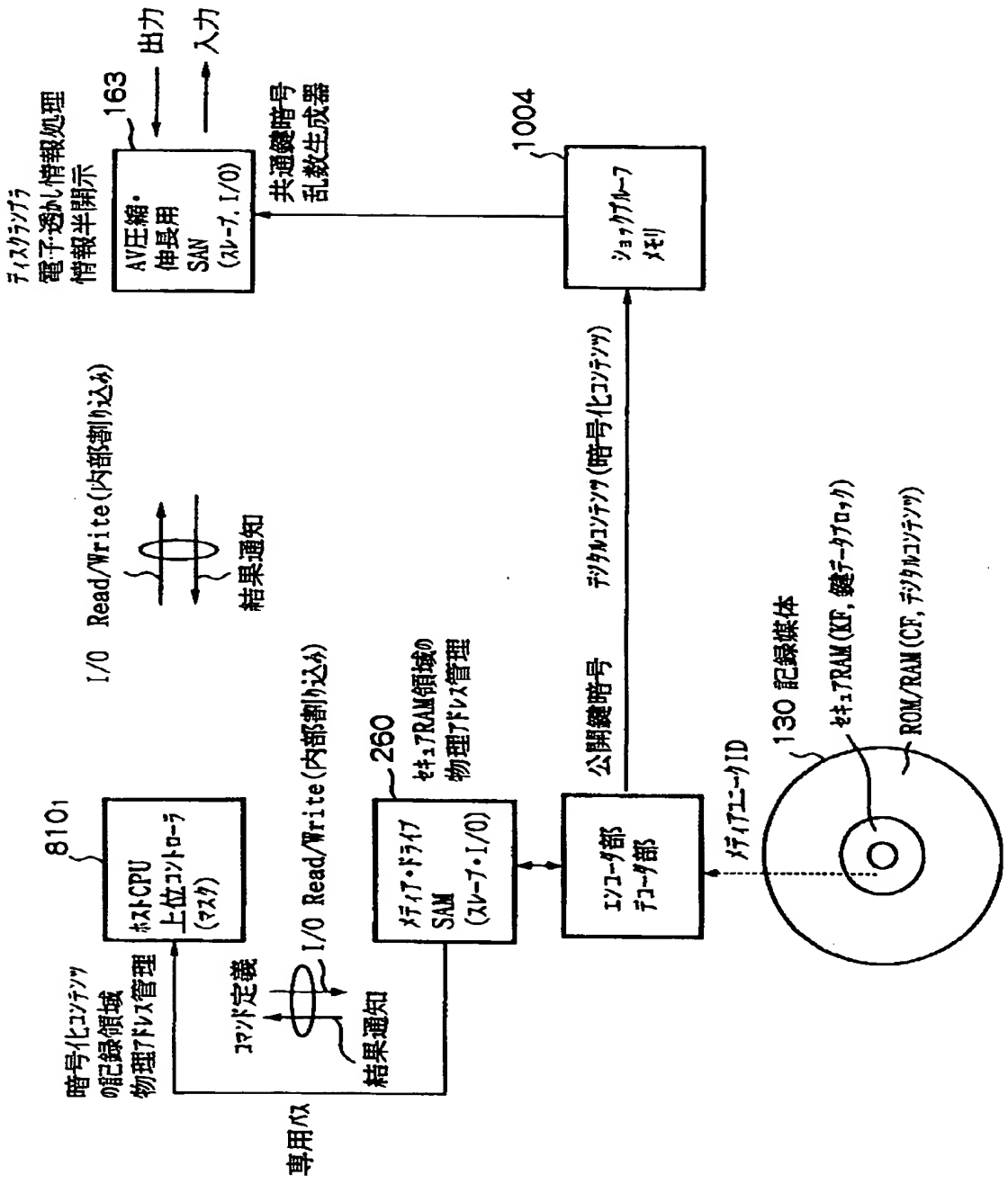
【図６５】


810₁
ホストCPU
上位コントローラ
(マスタ)
I/O Write
(内部割り込み)
結果通知
Suceed/False
①外部割り込み
②データホーリング
③I/O Read
105₁
SAM
(スレーブ, I/O)
デジタルコンテンツ
(暗号化コンテンツ)
鍵データブロック
メディアSAM 133
130 (スレーブ, I/O)
デジタルコンテンツ
(暗号化コンテンツ)

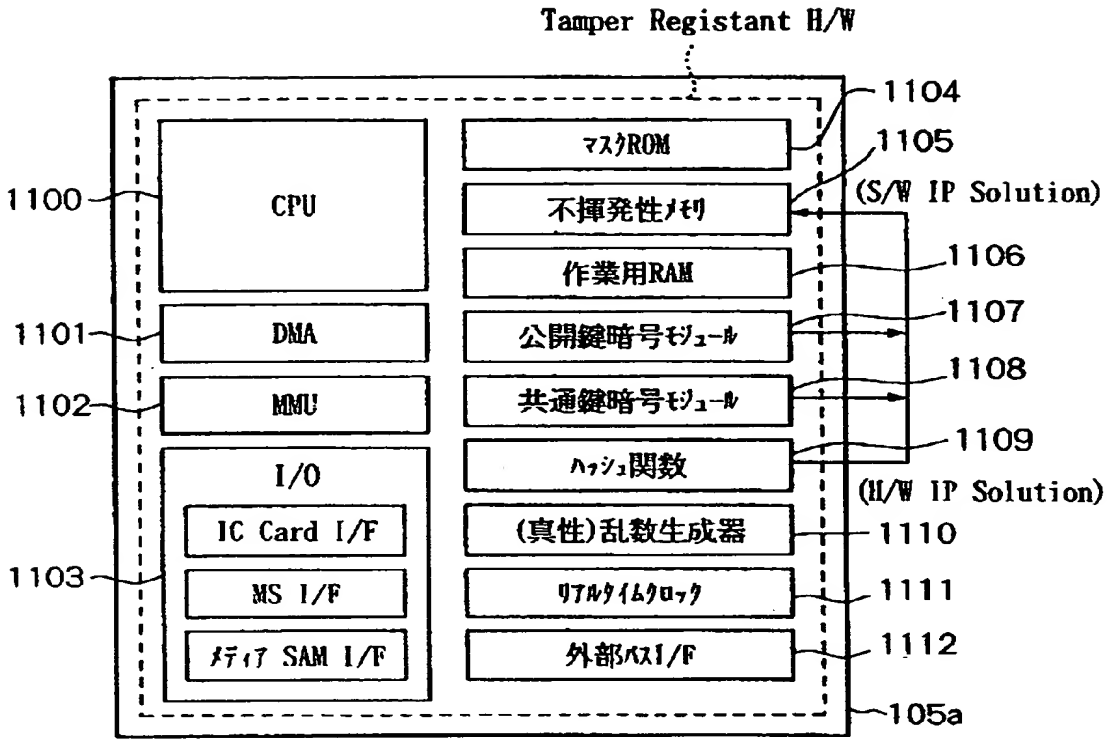
【図６６】


出力(再生)
入力(記録)
163
AV圧縮・伸長用SAM (スレーブ, I/O)
ディスクランプラ
電子透かしエンコーダ, デコーダ
デジタルコンテンツ (暗号化コンテンツ)
共通鍵暗号を利用した相互認証
コンテンツ鍵
130 (スレーブ, I/O)
鍵データブロック
記録媒体用セキュリティモジュール保存鍵
105
SAM (スレーブ, I/O)
課金情報 (利用履歴)
公開鍵暗号を利用した相互認証
メディアSAM
133
I/O Write (内部割り込み)
結果通知 Suceed/False
①外部割り込み
②データポーリング
③I/O Read
810
ホストCPU 上位コントローラ (マスタ)

【図６７】

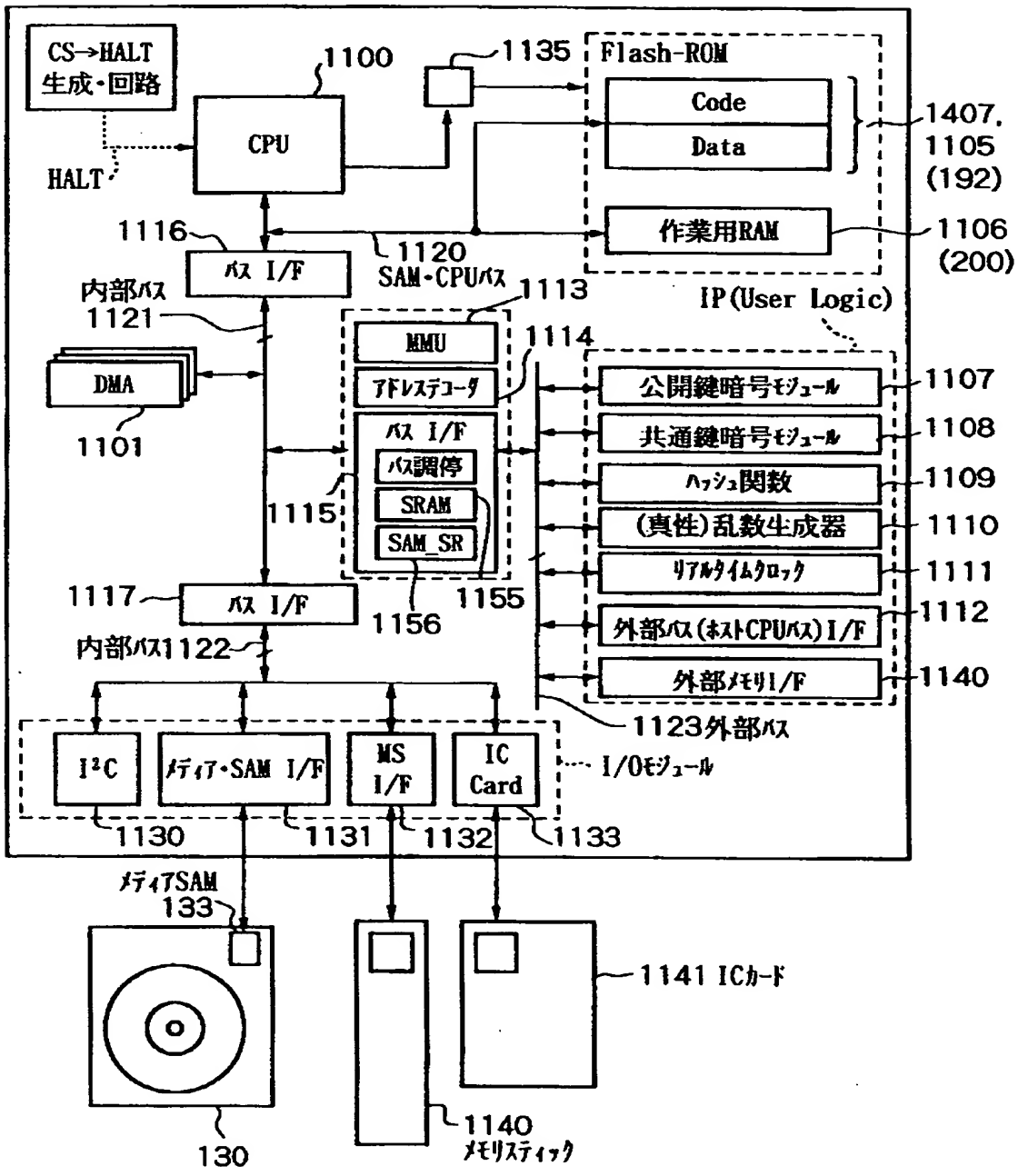

ディスクランプラ
電子透かし情報処理
情報半開示
163
出力
入力
AV圧縮・
伸長用
SAM
(スレーブ, I/O)
共通鍵暗号
乱数生成器
1004
シュックブルーフ
メモリ
I/O Read/Write(内部割り込み)
結果通知
8101
ホストCPU
上位コントローラ
(マスタ)
暗号化コンテンツ
の記録領域
物理アドレス管理
コマンド定義
I/O Read/Write(内部割り込み)
結果通知
専用バス
260
セキュアRAM領域の
物理アドレス管理
メディア・ドライブ
SAM
(スレーブ・I/O)
公開鍵暗号
デジタルコンテンツ(暗号化コンテンツ)
エンコーダ部
デコーダ部
メディアユニークID
130 記録媒体
セキュアRAM(XF, 鍵データブロック)
ROM/RAM(CF, デジタルコンテンツ)

【図６８】

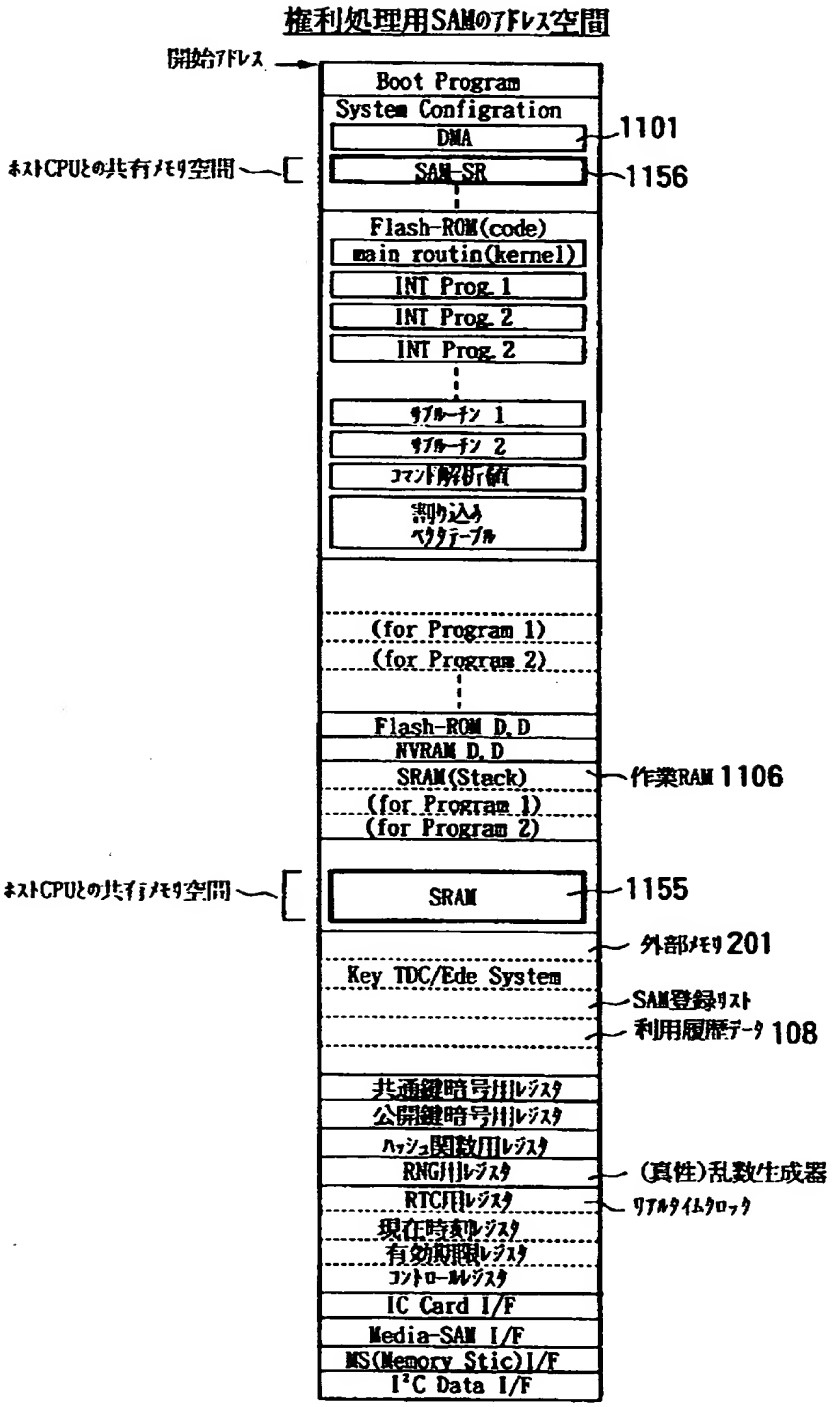


権利処理用のSAM105a

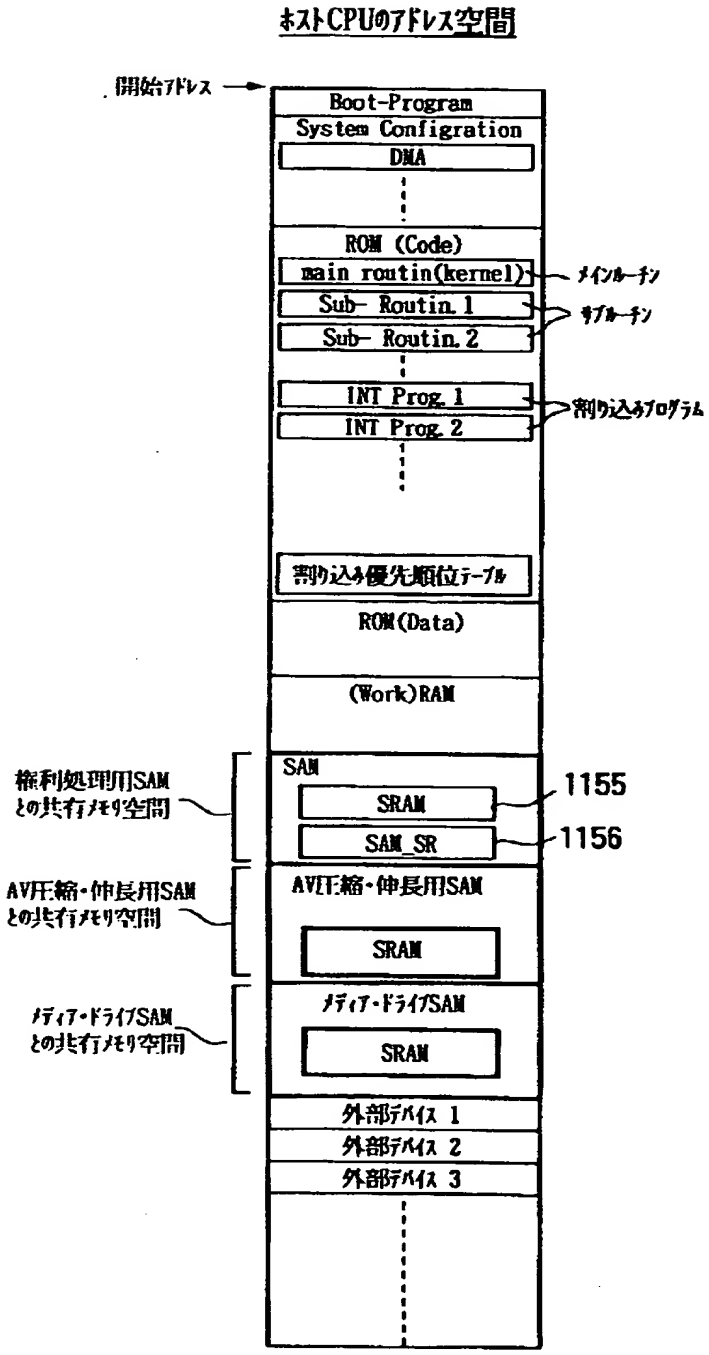
【図６９】


CS→HALT
生成・回路
HALT
1100
CPU
1135
Flash-ROM
Code
Data
1407,
1105
(192)
作業用RAM
1106
(200)
1116
バス I/F
1120
SAM-CPUバス
内部バス
1121
1113
IP(User Logic)
MMU
1114
アドレスデコーダ
DMA
1101
バス I/F
バス調停
SRAM
SAM_SR
1115
1155
1156
1117
バス I/F
内部バス1122
公開鍵暗号モジュール
1107
共通鍵暗号モジュール
1108
ハッシュ関数
1109
(真性)乱数生成器
1110
リアルタイムクロック
1111
外部バス(ホストCPUバス)I/F
1112
外部メモリI/F
1140
1123外部バス
I²C
メディア・SAM I/F
MS
I/F
IC
Card
I/Oモジュール
1130
1131
1132
1133
メディアSAM
133
1141 ICカード
130
1140
メモリスティック

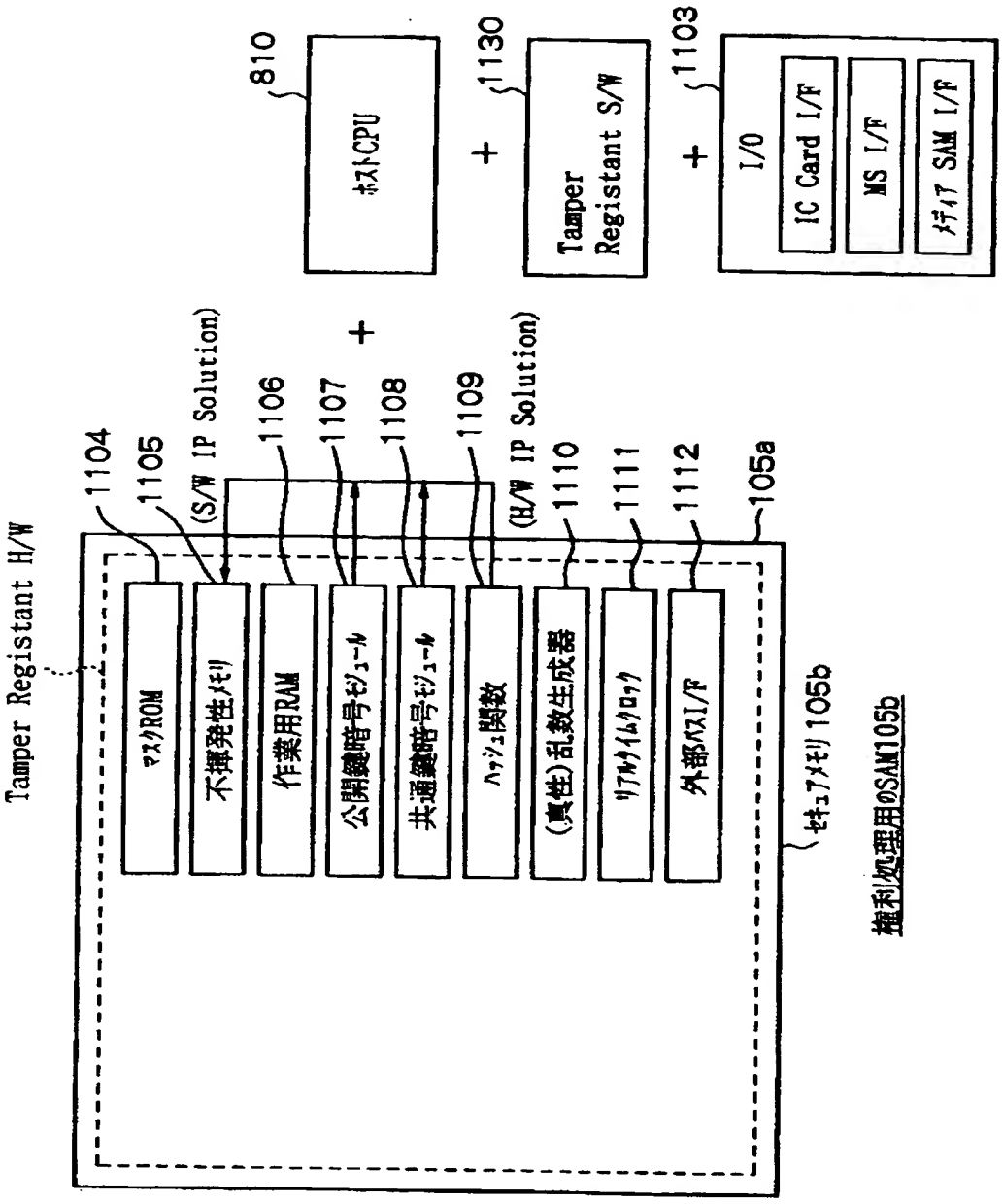
【図７０】


権利処理用SAMのアドレス空間
開始アドレス
Boot Program
System Configration
DMA
1101
ホストCPUとの共有メモリ空間
SAM_SR
1156
Flash-ROM(code)
main routin(kernel)
INT Prog. 1
INT Prog. 2
INT Prog. 2
サブルーチン 1
サブルーチン 2
コマンド解析部
割り込みベクタテーブル
(for Program 1)
(for Program 2)
Flash-ROM D.D
NVRAM D.D
SRAM(Stack)
作業RAM 1106
(for Program 1)
(for Program 2)
ホストCPUとの共有メモリ空間
SRAM
1155
外部メモリ 201
Key TDC/Ede System
SAM登録リスト
利用履歴データ 108
共通鍵暗号用レジスタ
公開鍵暗号用レジスタ
ハッシュ関数用レジスタ
RNG用レジスタ
(真性)乱数生成器
RTC用レジスタ
リアルタイムクロック
現在時刻レジスタ
有効期限レジスタ
コントロールレジスタ
IC Card I/F
Media-SAM I/F
MS(Memory Stic)I/F
I²C Data I/F

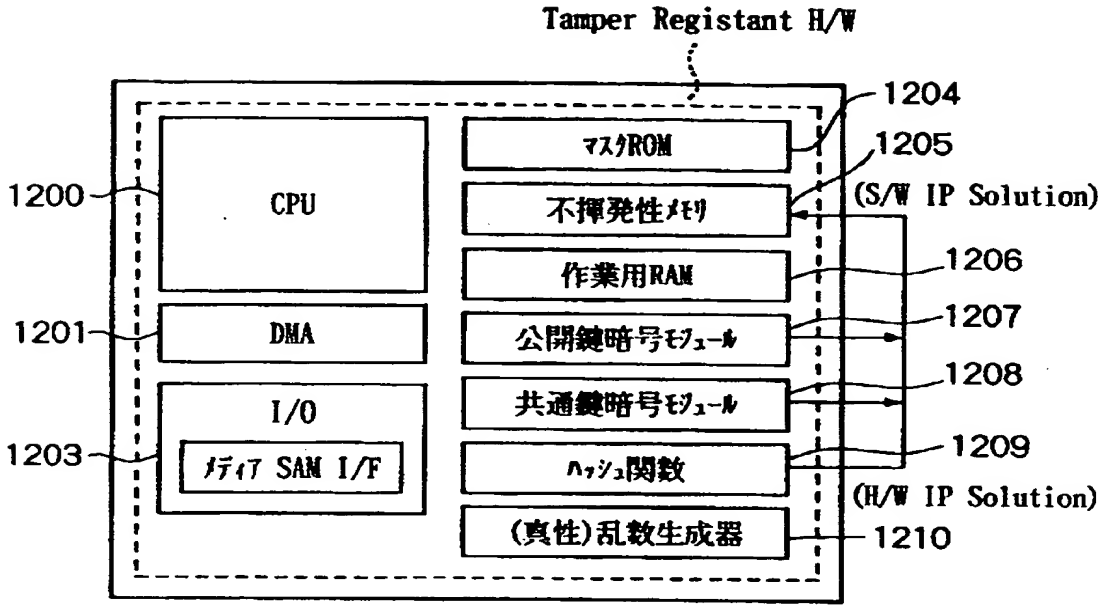
【図７１】


ホストCPUのアドレス空間
開始アドレス
Boot-Program
System Configration
DMA
ROM (Code)
main routin(kernel)
メインルーチン
Sub- Routin. 1
Sub- Routin. 2
サブルーチン
INT Prog. 1
INT Prog. 2
割り込みプログラム
割り込み優先順位テーブル
ROM(Data)
(Work)RAM
SAM
SRAM
1155
SAM_SR
1156
権利処理用SAM
との共有メモリ空間
AV圧縮・伸長用SAM
AV圧縮・伸長用SAM
との共有メモリ空間
SRAM
メディア・ドライブSAM
メディア・ドライブSAM
との共有メモリ空間
SRAM
外部デバイス 1
外部デバイス 2
外部デバイス 3

【図７２】

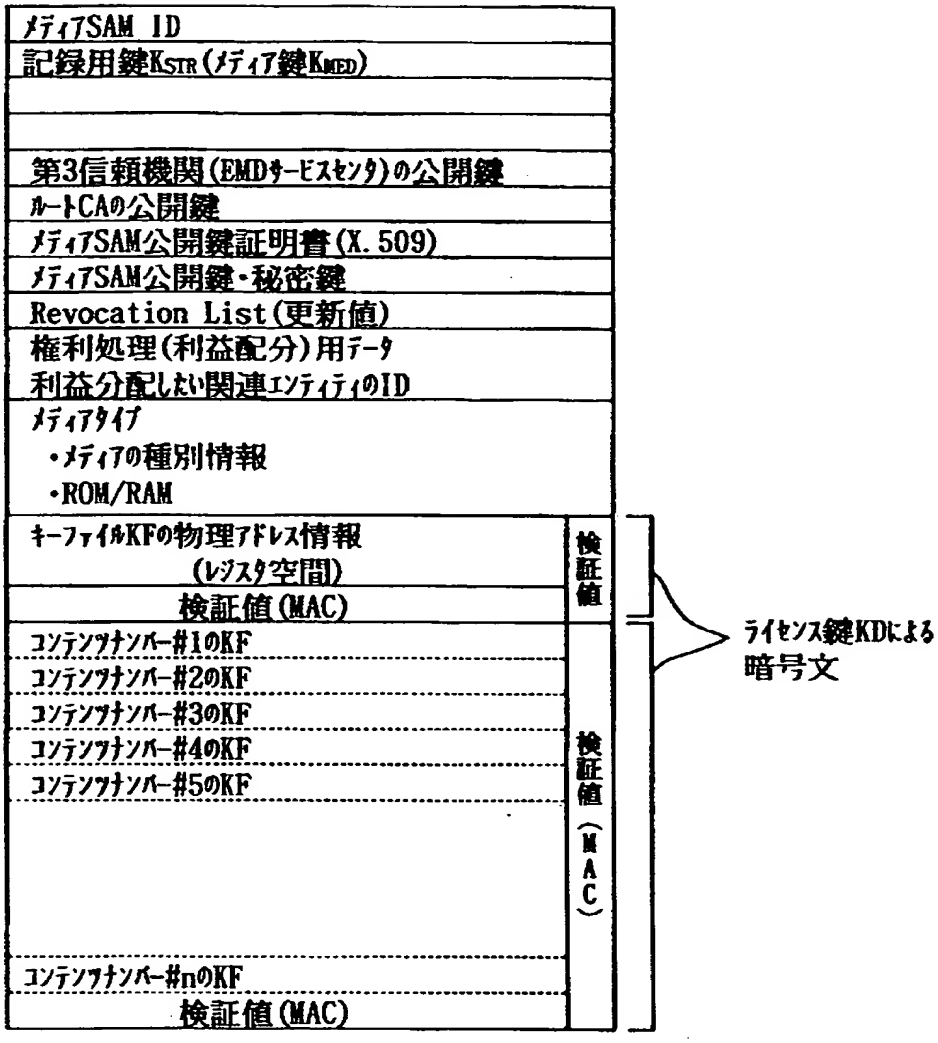

810
ホストCPU
+
1130
Tamper Registant S/W
+
1103
I/O
IC Card I/F
MS I/F
メディア SAM I/F
(S/W IP Solution)
(H/W IP Solution)
Tamper Registant H/W
1104
1105
1106
1107
1108
1109
1110
1111
1112
105a
マスクROM
不揮発性メモリ
作業用RAM
公開鍵暗号モジュール
共通鍵暗号モジュール
ハッシュ関数
(真性)乱数生成器
リアルタイムクロック
外部バスI/F
セキュアメモリ105b
権利処理用のSAM105b

【図７３】



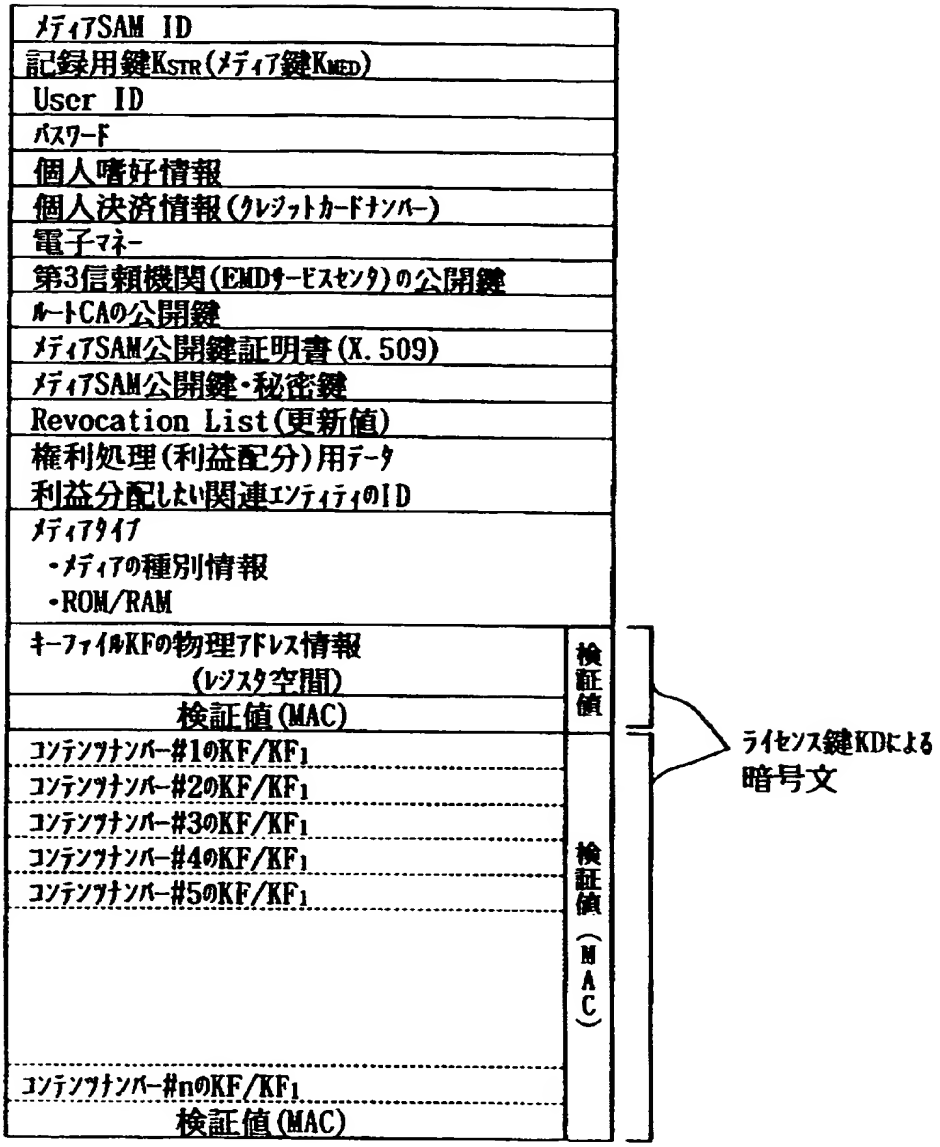
メディアSAM133a

【図７４】



ROM型の記録媒体のメディアSAMの記憶データ(出荷時)

【図７５】



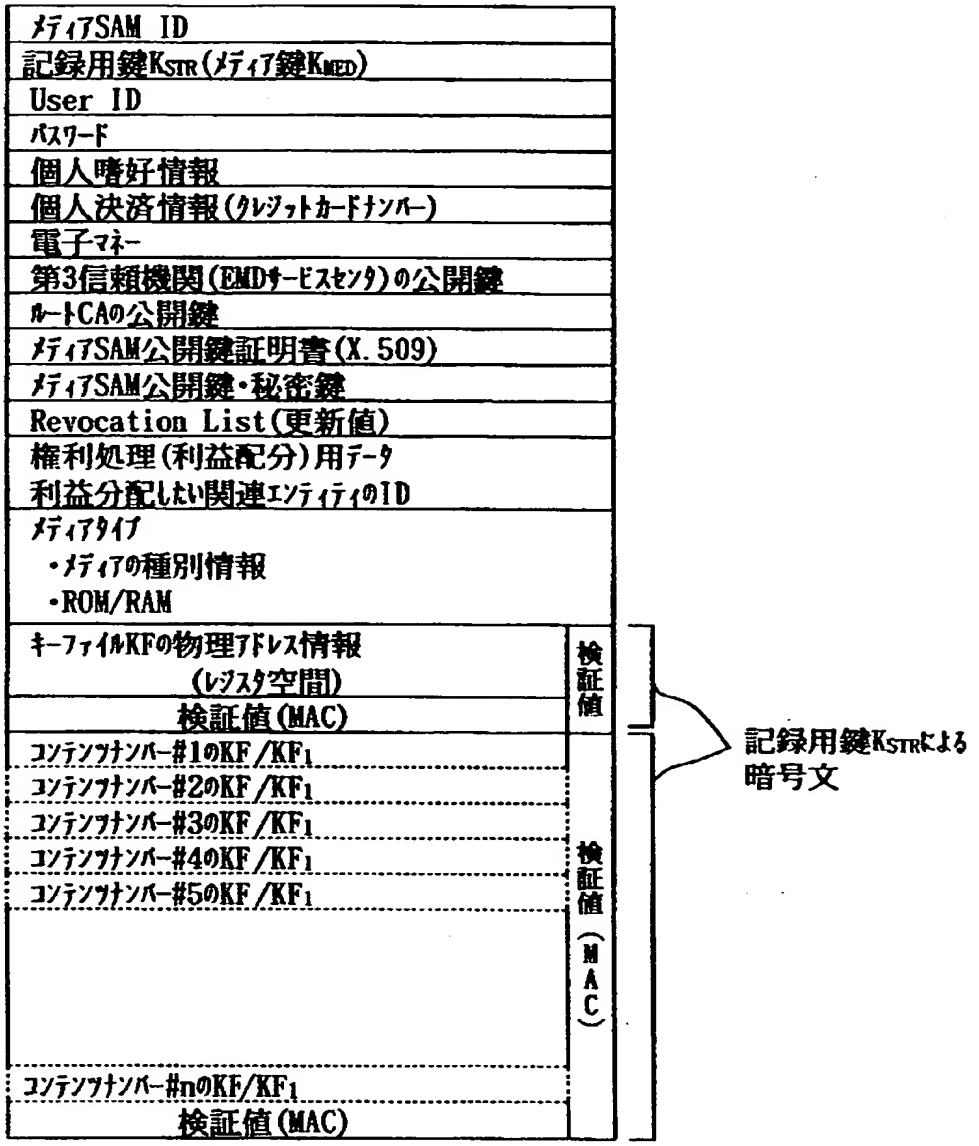
ROM型の記録媒体のメディアSAMの記憶データ(登録及び購入処理後)

【図７６】

メディアSAM ID
記録用鍵K_{STR}(メディア鍵K_{MED})
第3信頼機関(EMDサービスセンタ)の公開鍵
ルートCAの公開鍵
メディアSAM公開鍵証明書(X.509)
メディアSAM公開鍵・秘密鍵
Revocation List(更新値)
権利処理(利益配分)用データ 利益分配したい関連エンティティのID
メディアタイプ ・メディアの種別情報 ・ROM/RAM

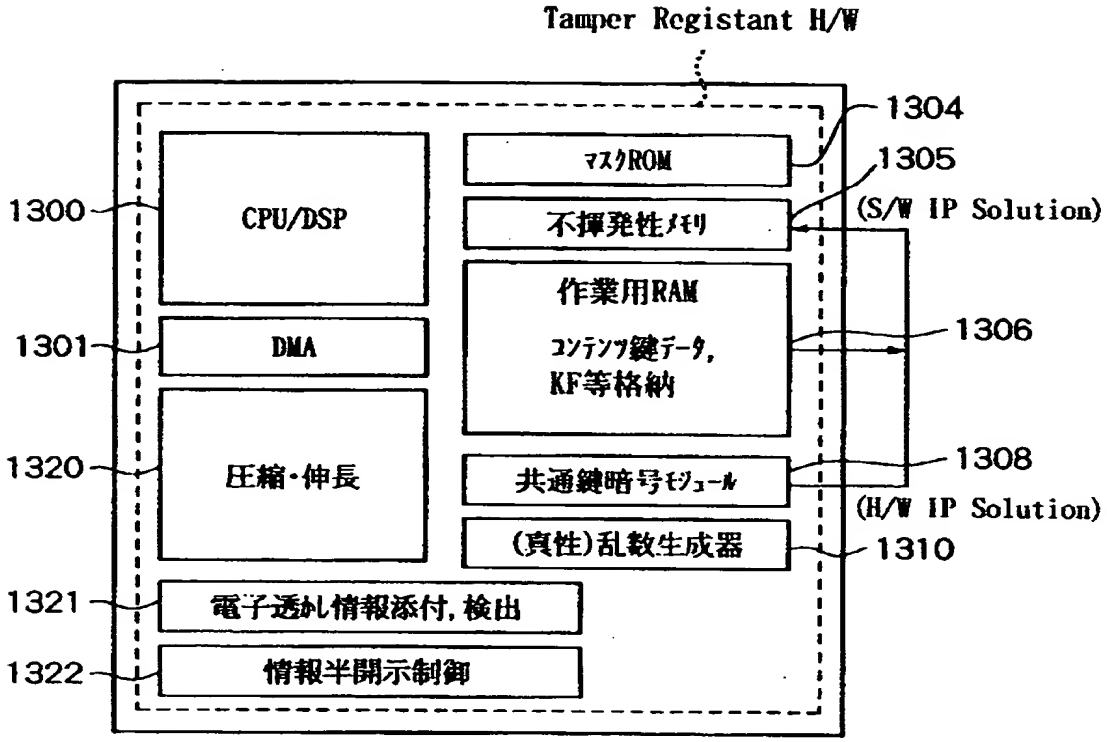
RAMの記録媒体のメディアSAMの記憶データ(出荷時)

【図７７】



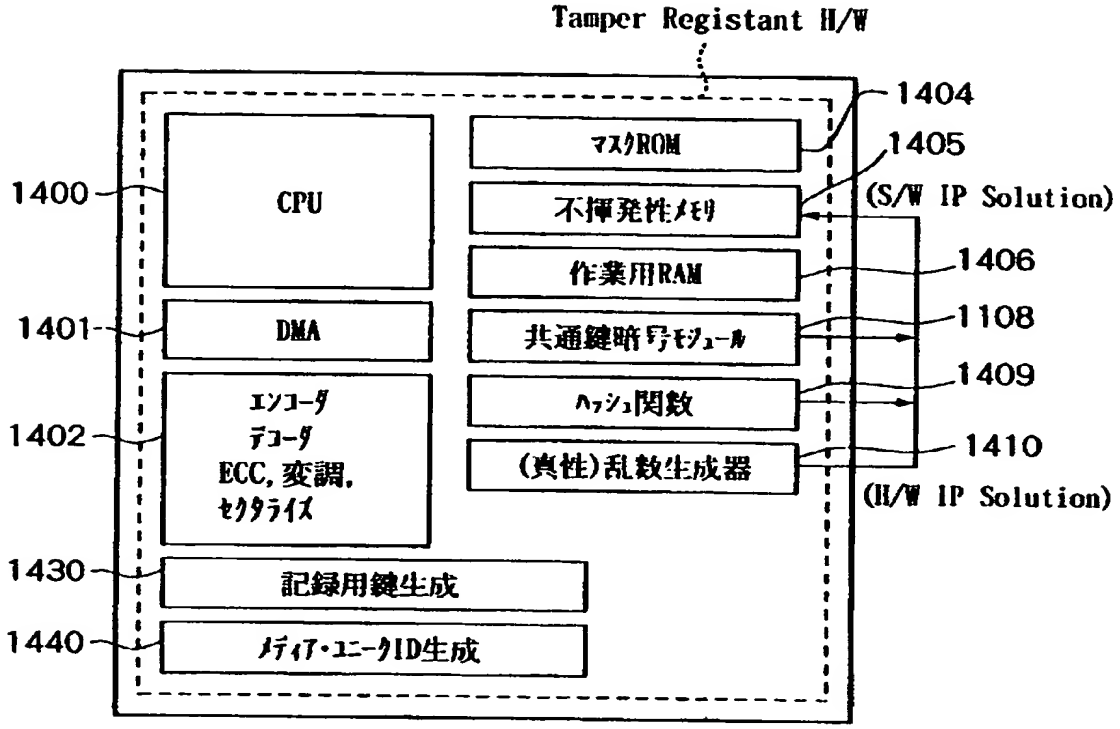
RAMの記録媒体のメディアSAMの記憶データ(登録及び購入処理後)

【図７８】



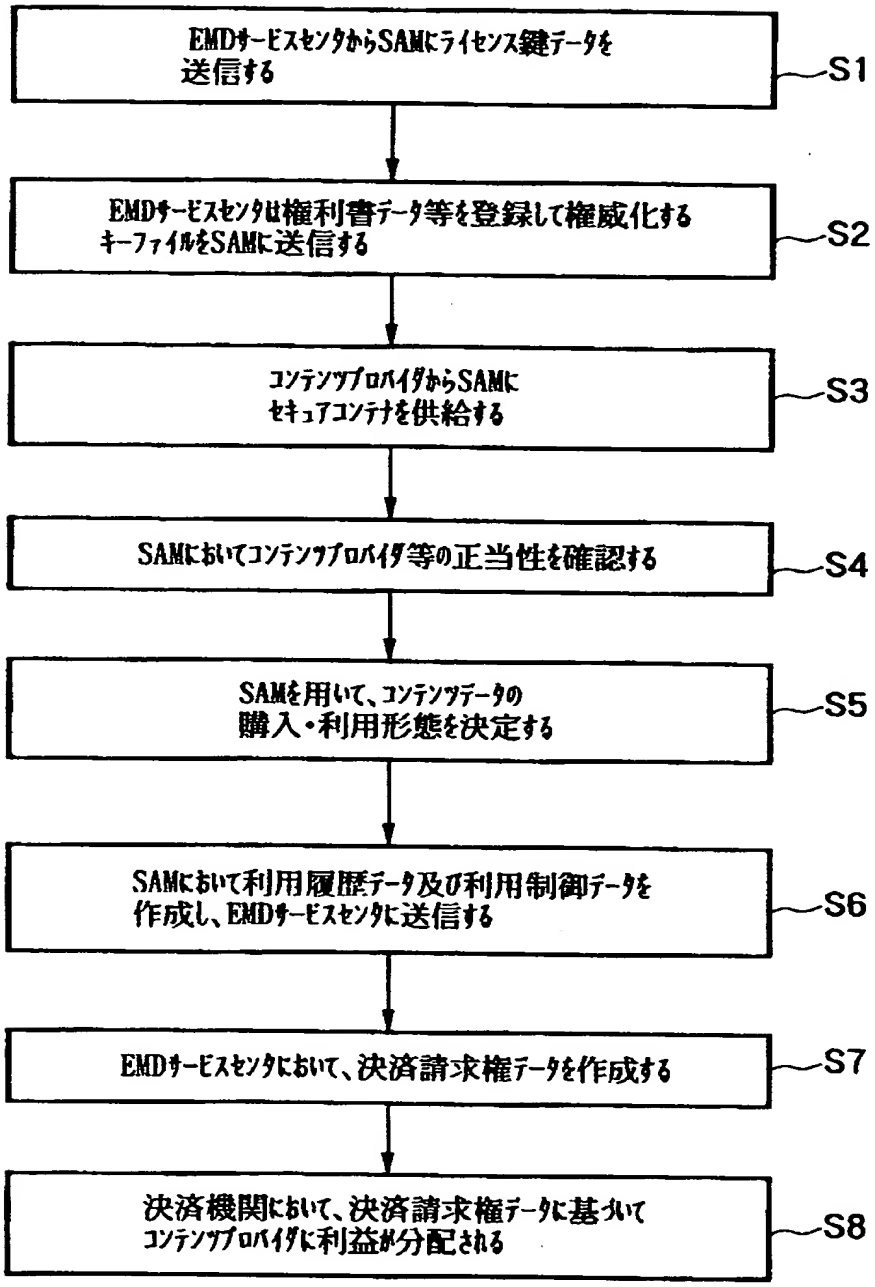
AV圧縮・伸長用SAM163

【図７９】

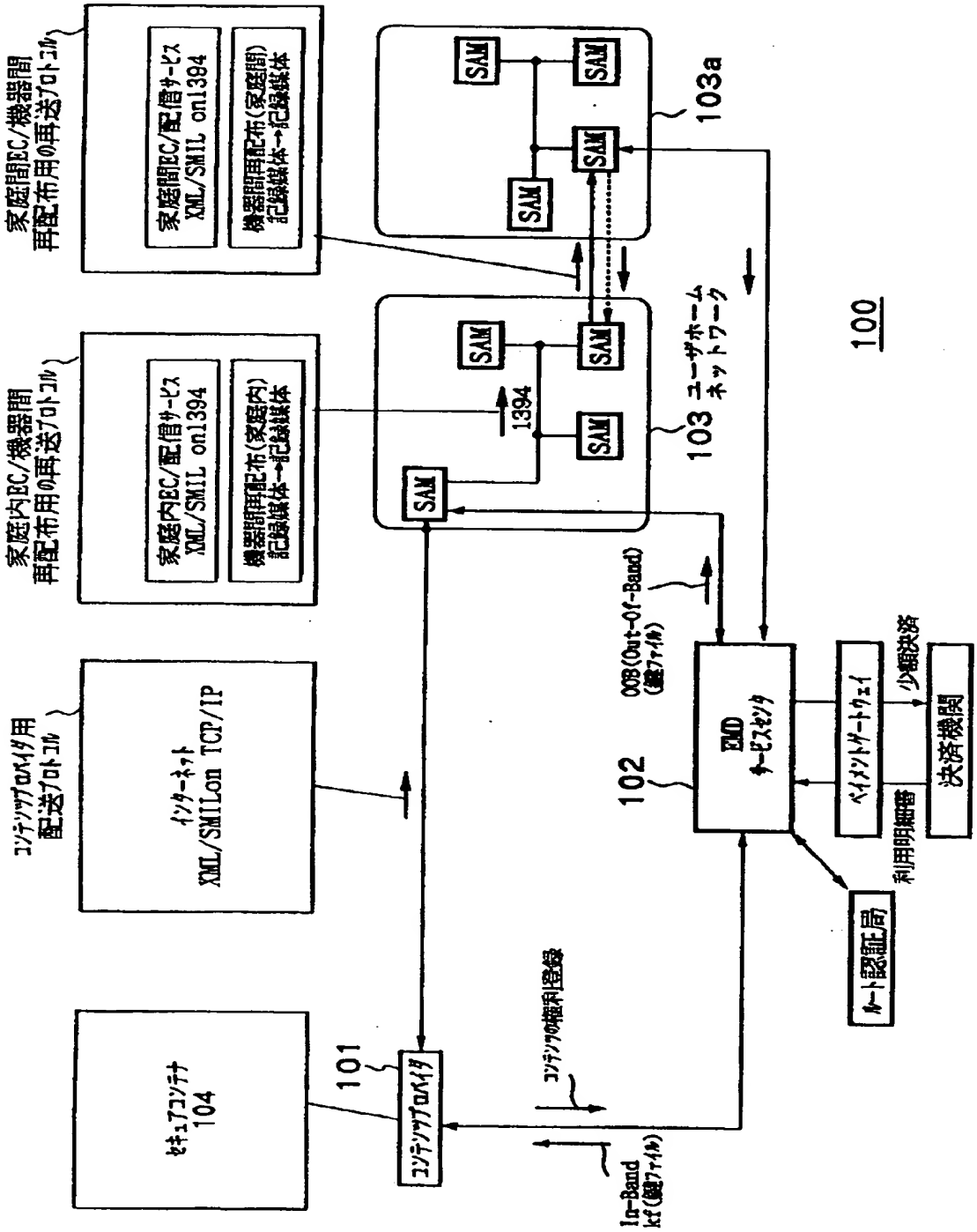


メディア・ドライブSAM260a

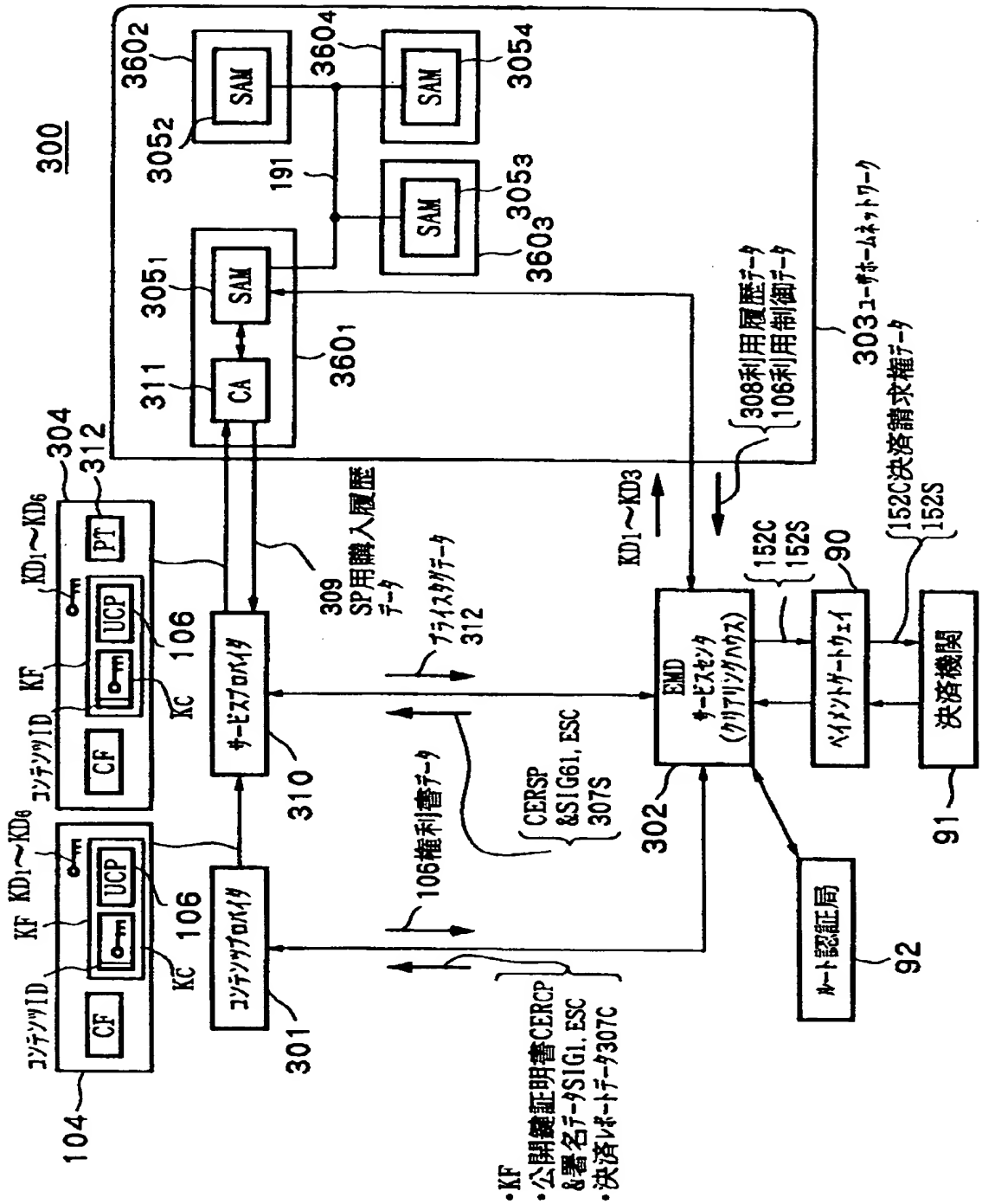
【図８０】


EMDサービスセンタからSAMにライセンス鍵データを送信する
S1
EMDサービスセンタは権利書データ等を登録して権威化するキーファイルをSAMに送信する
S2
コンテンツプロバイダからSAMにセキュアコンテナを供給する
S3
SAMにおいてコンテンツプロバイダ等の正当性を確認する
S4
SAMを用いて、コンテンツデータの購入・利用形態を決定する
S5
SAMにおいて利用履歴データ及び利用制御データを作成し、EMDサービスセンタに送信する
S6
EMDサービスセンタにおいて、決済請求権データを作成する
S7
決済機関において、決済請求権データに基づいてコンテンツプロバイダに利益が分配される
S8

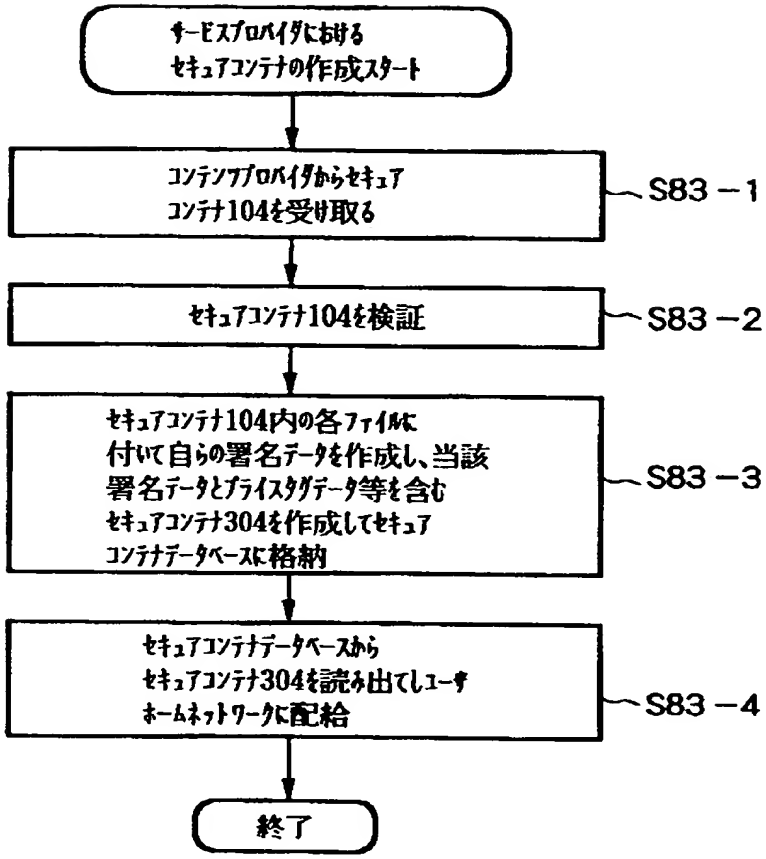
【図８１】


家庭間EC/機器間
再配布用の再送プロトコル
家庭間EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭間)
記録媒体→記録媒体
家庭内EC/機器間
再配布用の再送プロトコル
家庭内EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭内)
記録媒体→記録媒体
コンテンツプロバイダ用
配送プロトコル
インターネット
XML/SMILon TCP/IP
セキュアコンテナ
104
101
コンテンツプロバイダ
コンテンツの権利登録
In-Band
kf(鍵ファイル)
SAM
1394
103
ユーザホーム
ネットワーク
103a
100
102
EMD
サービスセンタ
OOB(Out-Of-Band)
(鍵ファイル)
ペイメントゲートウェイ
少額決済
決済機関
利用明細書
ルート認証局

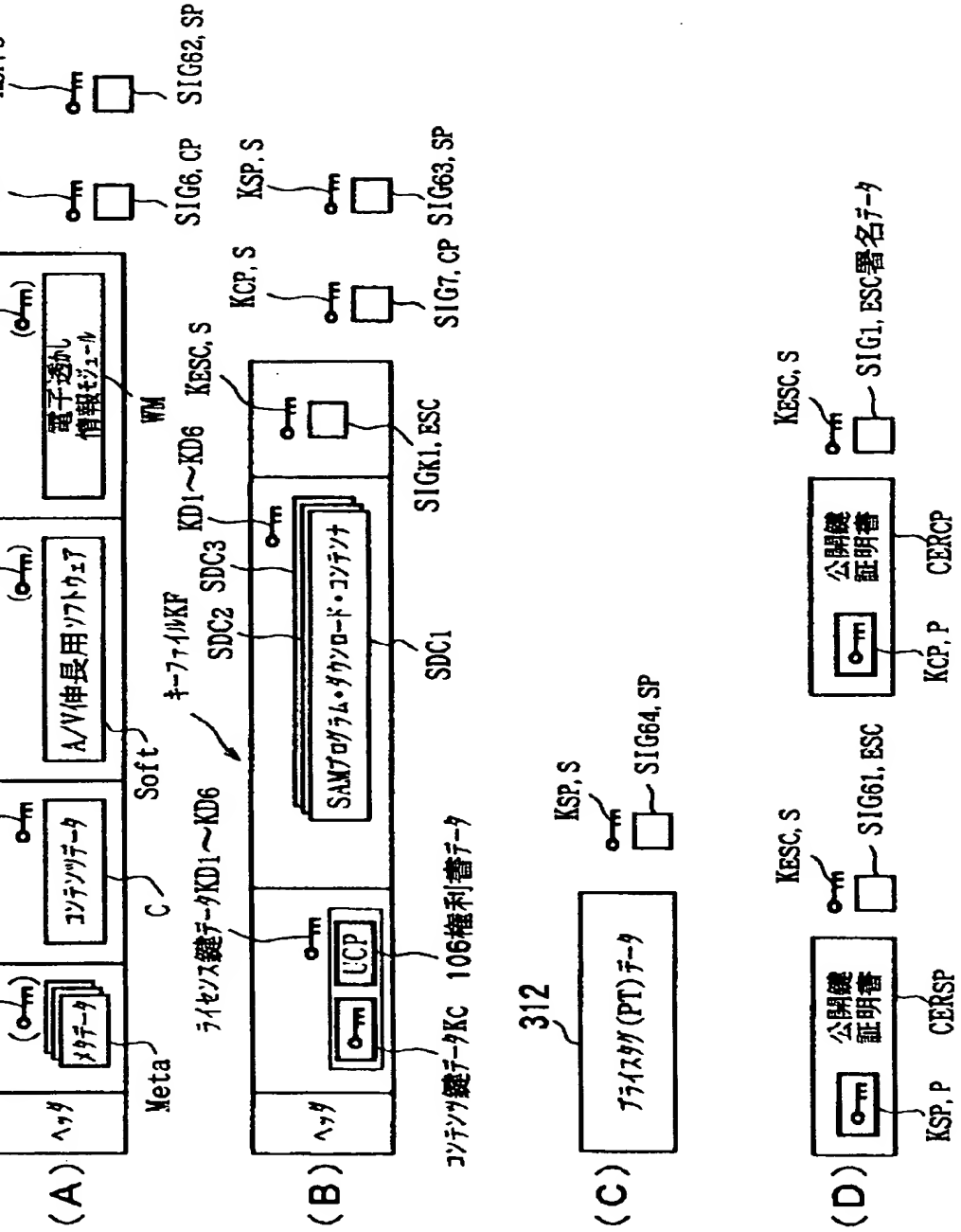
【図８２】


300
SAM
CA
CF
UCP
PT
KF
KC
KD1～KD6
KD1～KD3
106
310
301
302
304
312
311
191
309 SP用購入履歴データ
312 プライスタグデータ
106権利書データ
CERSP &SIG1, ESC 307S
152C 152S
90
91
92
152C決済請求権データ
152S
308利用履歴データ
106利用制御データ
303
サービスセンタ (クリアリングハウス)
ペイメントゲートウェイ
決済機関
カード認証局
コンテンツID
コンテンツプロバイダ
サービスプロバイダ
104
・KF
・公開鍵証明書CERCP &署名データSIG1, ESC
・決済レポートデータ307C

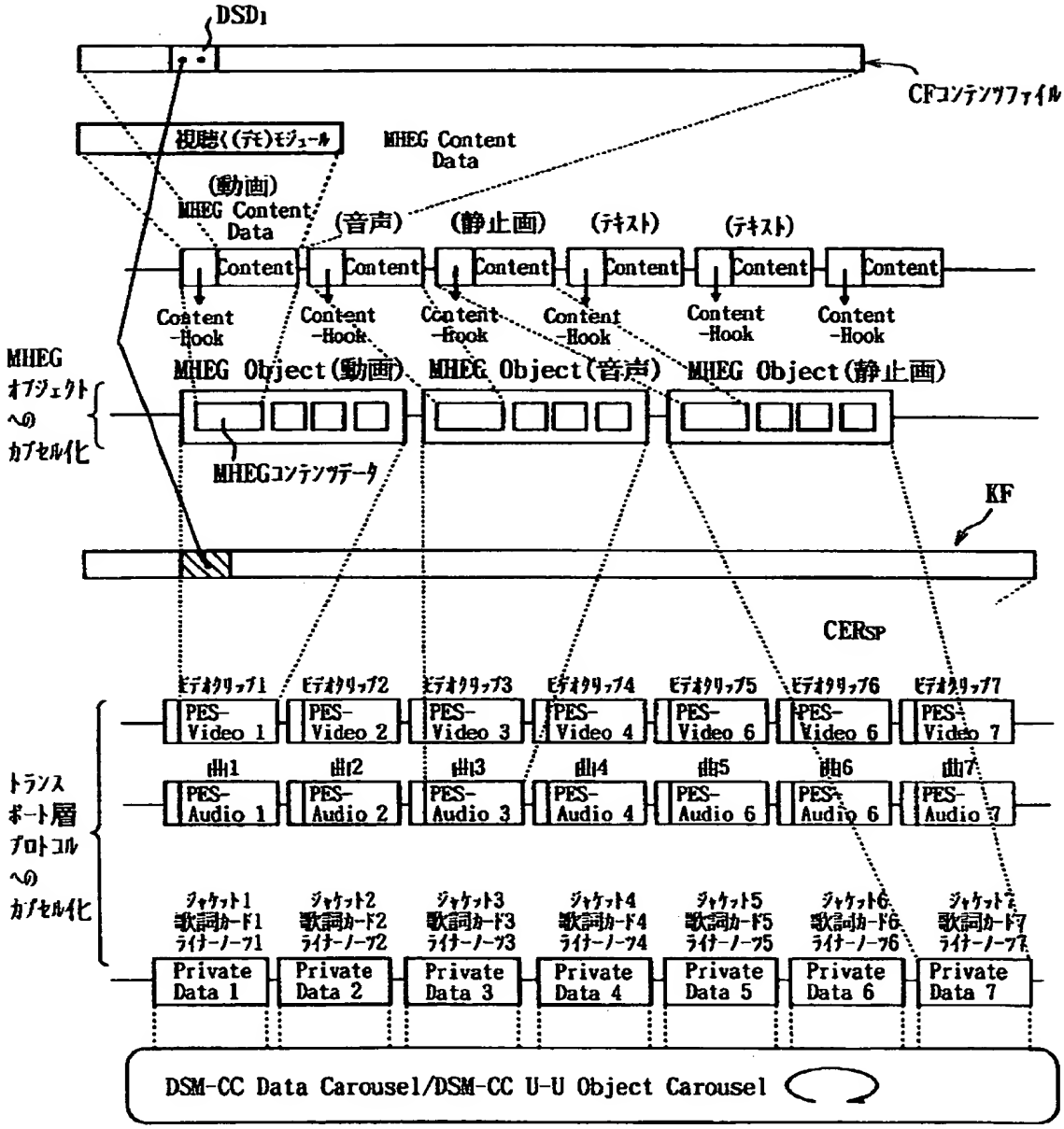
【図８３】


サービスプロバイダにおける
セキュアコンテナの作成スタート
コンテンツプロバイダからセキュア
コンテナ104を受け取る
S83－1
セキュアコンテナ104を検証
S83－2
セキュアコンテナ104内の各ファイルに
付いて自らの署名データを作成し、当該
署名データとプライスタグデータ等を含む
セキュアコンテナ304を作成してセキュア
コンテナデータベースに格納
S83－3
セキュアコンテナデータベースから
セキュアコンテナ304を読み出してユーザ
ホームネットワークに配給
S83－4
終了

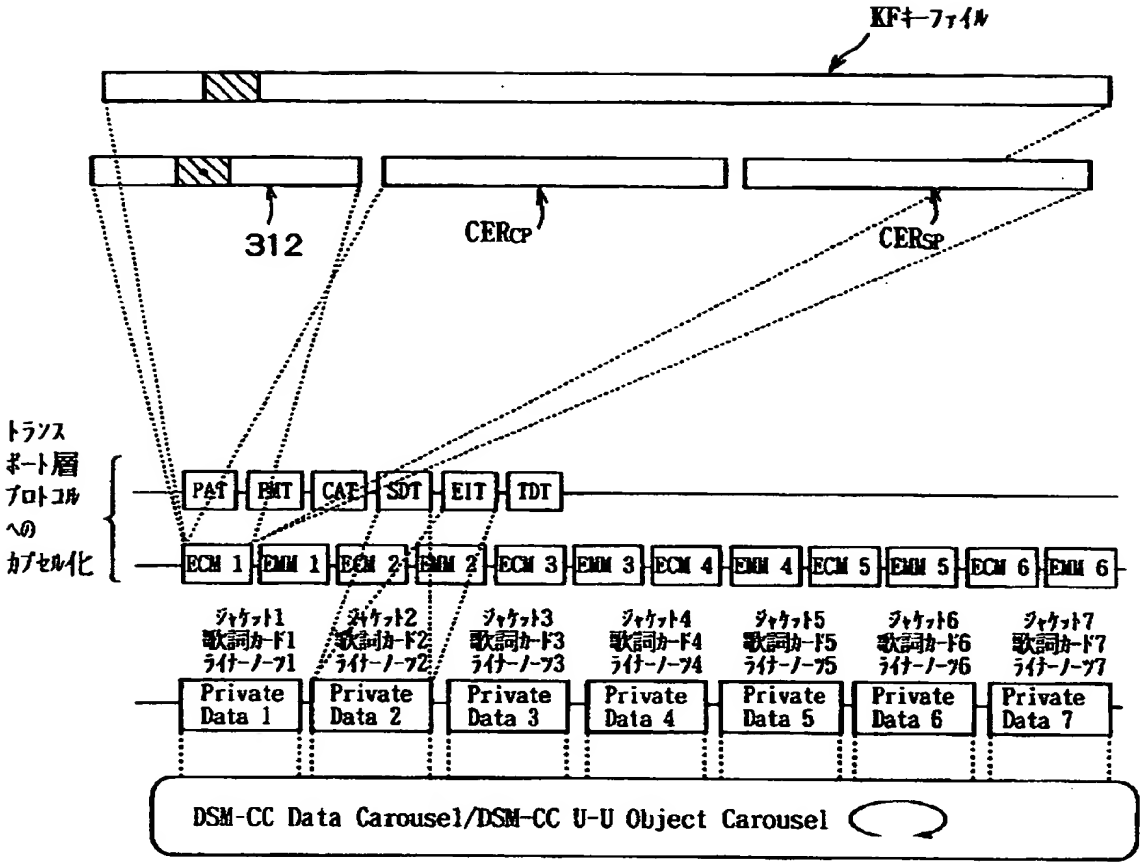
【図８４】


304セキュアコンテナ
コンテンツファイルCF
KC
KCP, S
KSP, S
SIG62, SP
SIG6, CP
電子透かし情報モジュール
WM
A/V伸長用ソフトウェア
Soft
コンテンツデータ
C
メタデータ
Meta
コンテンツ鍵データKC
ライセンス鍵データKD1～KD6
KESC, S
KD1～KD6
SIG7, CP
SIG63, SP
SIGK1, ESC
キーファイルKF
SDC2
SDC3
SAMプログラム・ダウンロード・コンテンツ
SDC1
UCP
コンテンツ鍵データKC
106権利書データ
312
プライスタグ(PT)データ
SIG64, SP
SIG61, ESC
SIG1, ESC署名データ
公開鍵証明書
CERCP
CERSP
KCP, P
KSP, P
(A)
(B)
(C)
(D)

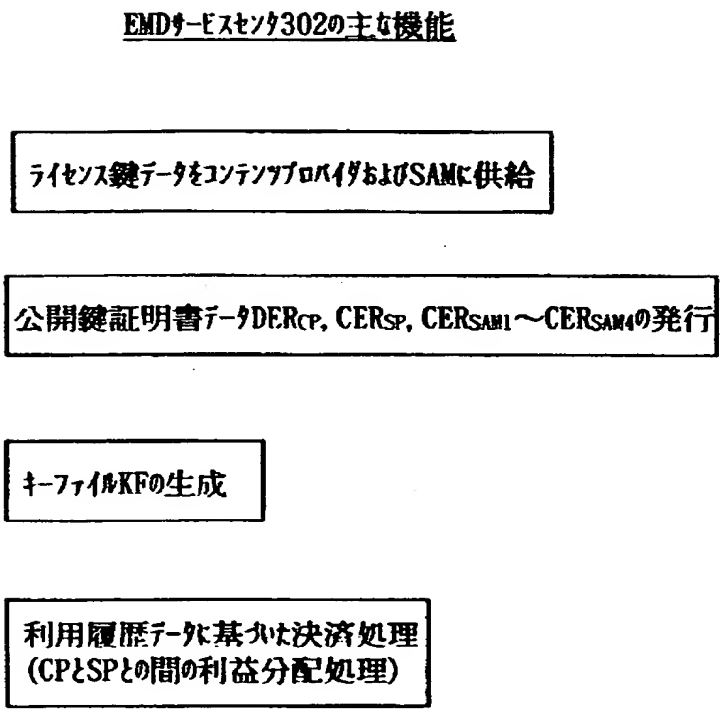
【図８５】


DSD1
CFコンテンツファイル
視聴(デモ)モジュール
MHEG Content Data
(動画)
MHEG Content Data
(音声)
(静止画)
(テキスト)
(テキスト)
Content
Content-Hook
MHEG オブジェクトへのカプセル化
MHEG Object(動画)
MHEG Object(音声)
MHEG Object(静止画)
MHEGコンテンツデータ
KF
CERSP
ビデオクリップ1
ビデオクリップ2
ビデオクリップ3
ビデオクリップ4
ビデオクリップ5
ビデオクリップ6
ビデオクリップ7
PES-Video 1
PES-Video 2
PES-Video 3
PES-Video 4
PES-Video 6
PES-Video 6
PES-Video 7
曲1
曲2
曲3
曲4
曲5
曲6
曲7
PES-Audio 1
PES-Audio 2
PES-Audio 3
PES-Audio 4
PES-Audio 6
PES-Audio 6
PES-Audio 7
トランスポート層プロトコルへのカプセル化
ジャケット1 歌詞カード1 ライナーノーツ1
ジャケット2 歌詞カード2 ライナーノーツ2
ジャケット3 歌詞カード3 ライナーノーツ3
ジャケット4 歌詞カード4 ライナーノーツ4
ジャケット5 歌詞カード5 ライナーノーツ5
ジャケット6 歌詞カード6 ライナーノーツ6
ジャケット7 歌詞カード7 ライナーノーツ7
Private Data 1
Private Data 2
Private Data 3
Private Data 4
Private Data 5
Private Data 6
Private Data 7
DSM-CC Data Carousel/DSM-CC U-U Object Carousel

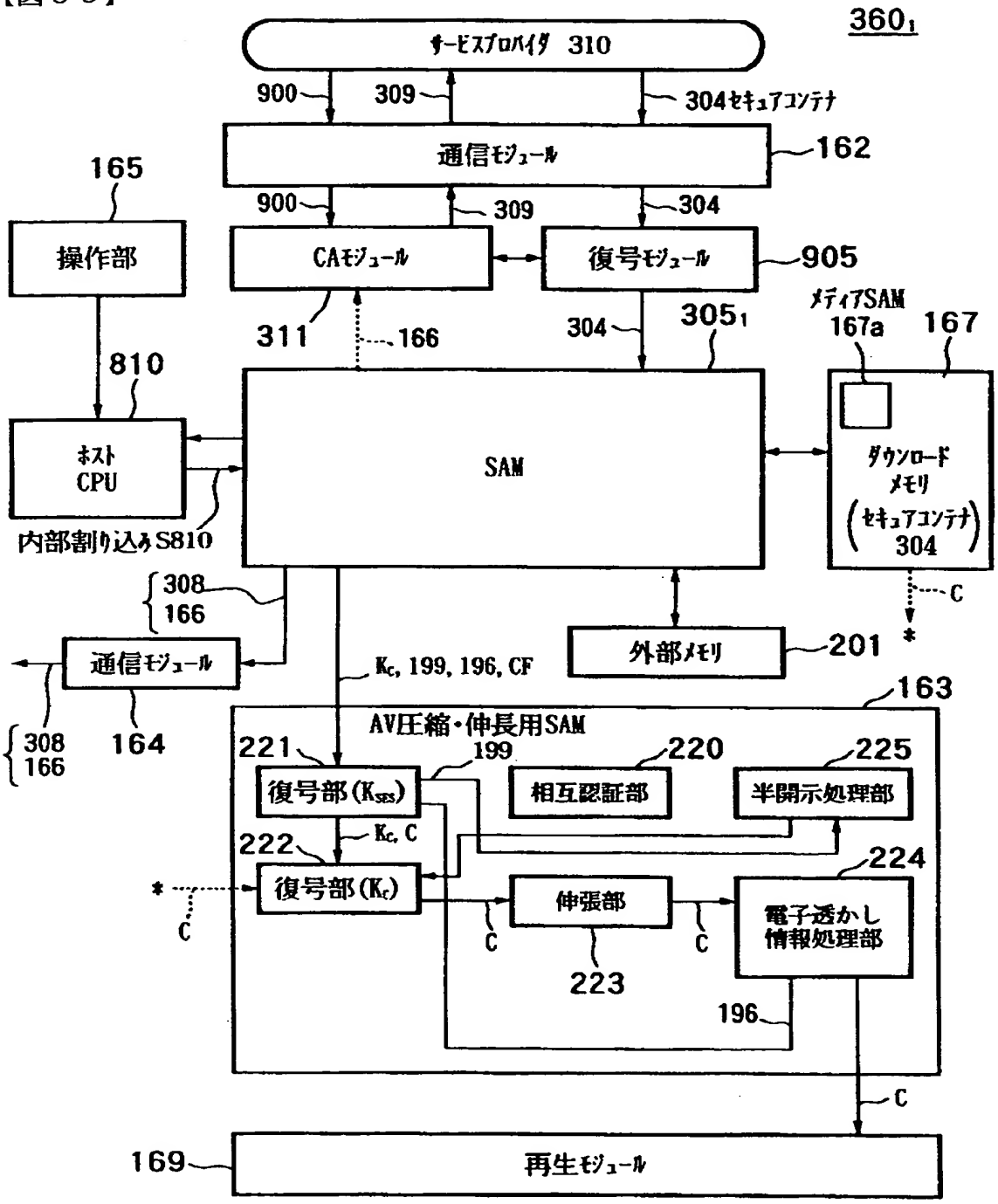
【図８６】


KFキーファイル
312
CERCP
CERSP
トランスポート層プロトコルへのカプセル化
PAT
PMT
CAT
SDT
EIT
TDT
ECM 1
EMM 1
ECM 2
EMM 2
ECM 3
EMM 3
ECM 4
EMM 4
ECM 5
EMM 5
ECM 6
EMM 6
ジャケット1 歌詞カード1 ライナーノーツ1
ジャケット2 歌詞カード2 ライナーノーツ2
ジャケット3 歌詞カード3 ライナーノーツ3
ジャケット4 歌詞カード4 ライナーノーツ4
ジャケット5 歌詞カード5 ライナーノーツ5
ジャケット6 歌詞カード6 ライナーノーツ6
ジャケット7 歌詞カード7 ライナーノーツ7
Private Data 1
Private Data 2
Private Data 3
Private Data 4
Private Data 5
Private Data 6
Private Data 7
DSM-CC Data Carousel/DSM-CC U-U Object Carousel

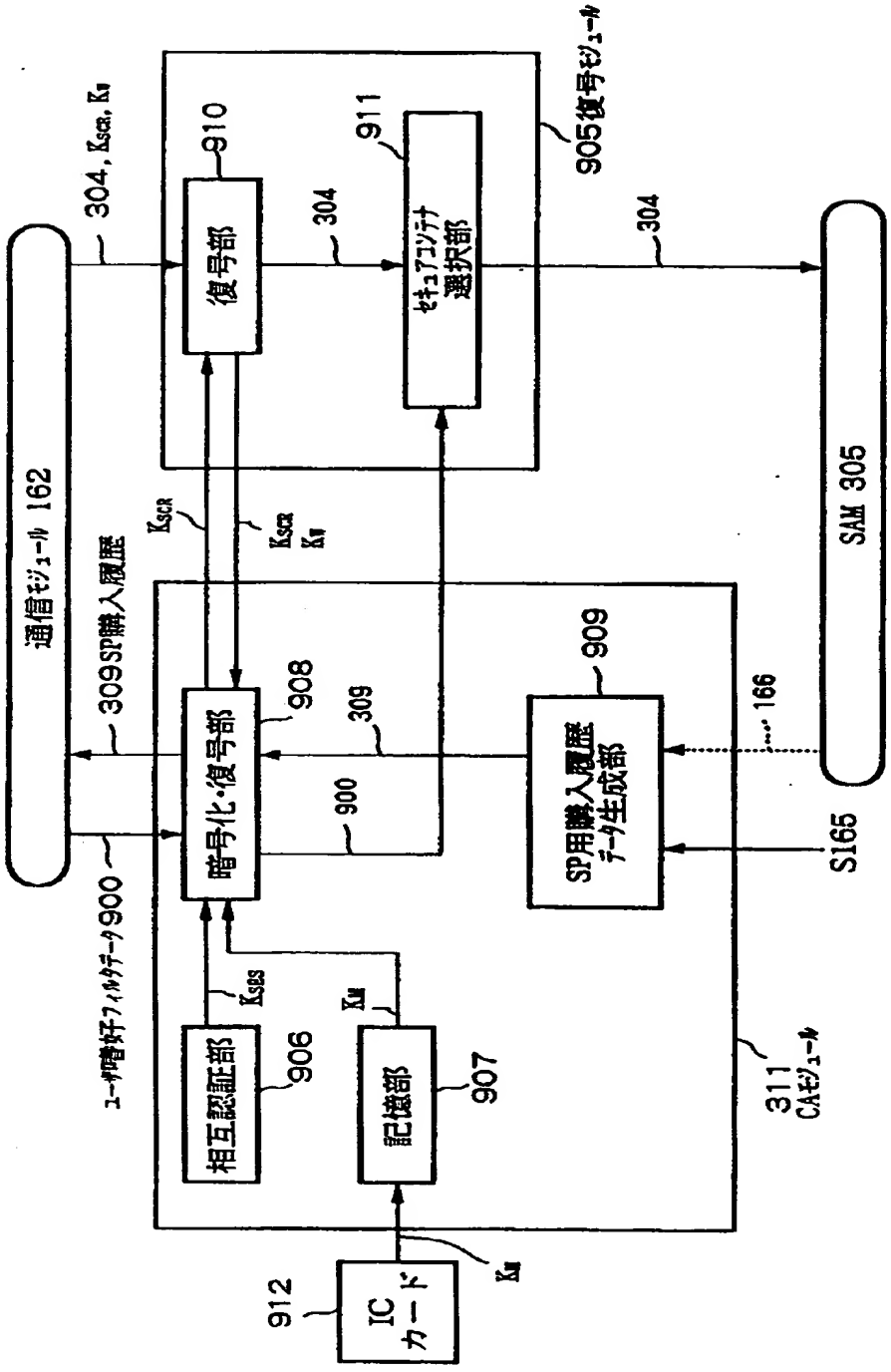
【図８７】


EMDサービスセンタ302の主な機能
ライセンス鍵データをコンテンツプロバイダおよびSAMに供給
公開鍵証明書データDERCP, CERSP, CERSAM1～CERSAM4の発行
キーファイルKFの生成
利用履歴データに基づいた決済処理
(CPとSPとの間の利益分配処理)

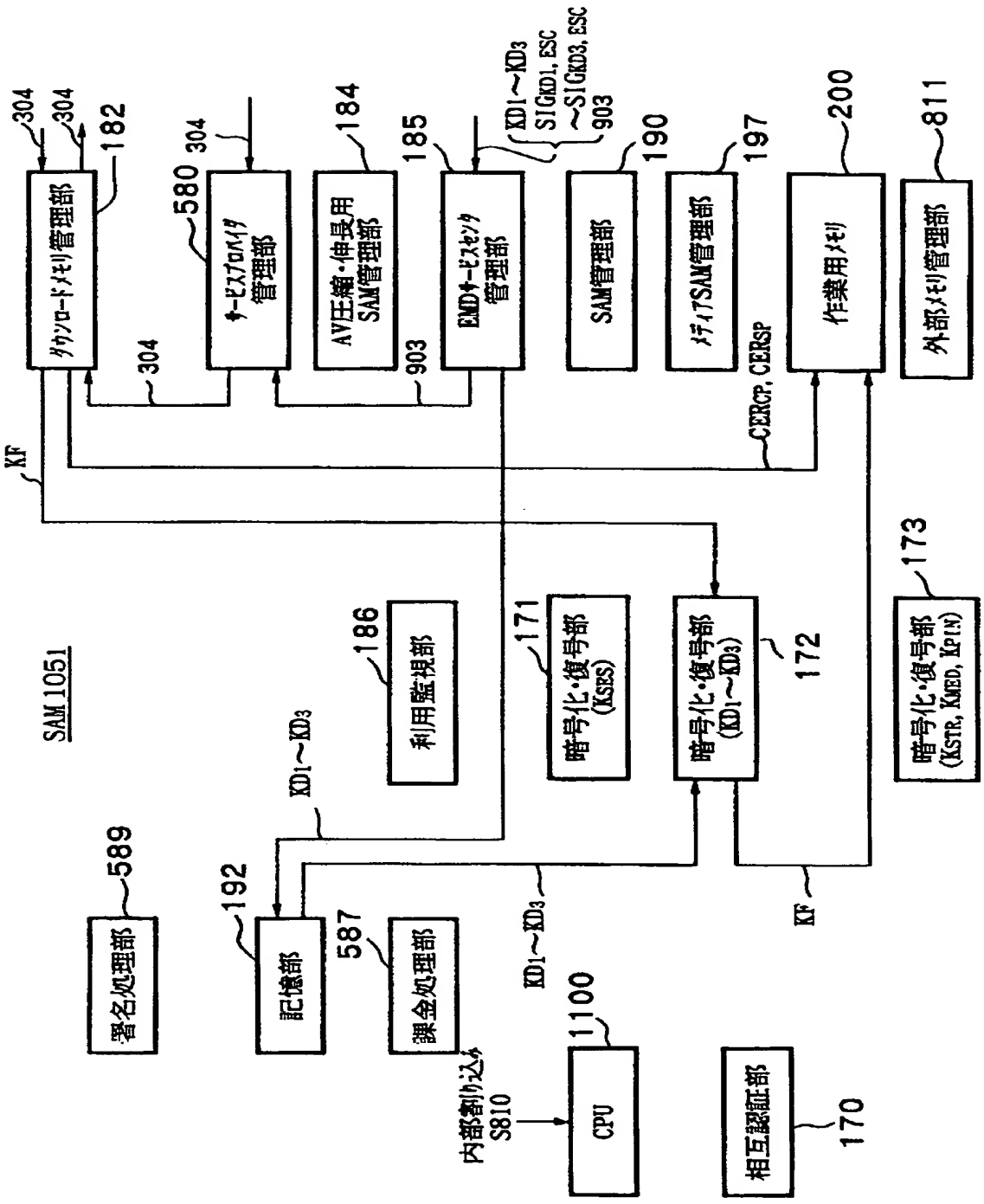
【図８８】


360₁
サービスプロバイダ 310
900
309
304セキュアコンテナ
通信モジュール
162
165
操作部
900
309
304
CAモジュール
復号モジュール
905
311
166
304
305₁
メディアSAM
167a
167
810
ホスト
CPU
SAM
ダウンロード
メモリ
(セキュアコンテナ
304)
内部割り込みS810
308
166
C
通信モジュール
Kc, 199, 196, CF
外部メモリ
201
163
AV圧縮・伸長用SAM
308
166
164
221
199
220
225
復号部(Kscs)
相互認証部
半開示処理部
222
Kc, C
224
復号部(Kc)
伸張部
電子透かし
情報処理部
C
C
C
223
196
C
169
再生モジュール

【図８９】


通信モジュール 162
304, Kscr, Ks
復号部
910
911
セキュアコンテナ選択部
905復号モジュール
304
304
SAM 305
Kscr
Kscr
Ks
309SP購入履歴
暗号化・復号部
908
309
900
SP用購入履歴データ生成部
909
166
S165
ユーザ嗜好フィルタデータ900
Kses
Ku
相互認証部
906
記憶部
907
311
CAモジュール
912
ICカード
Ku

【図９０】

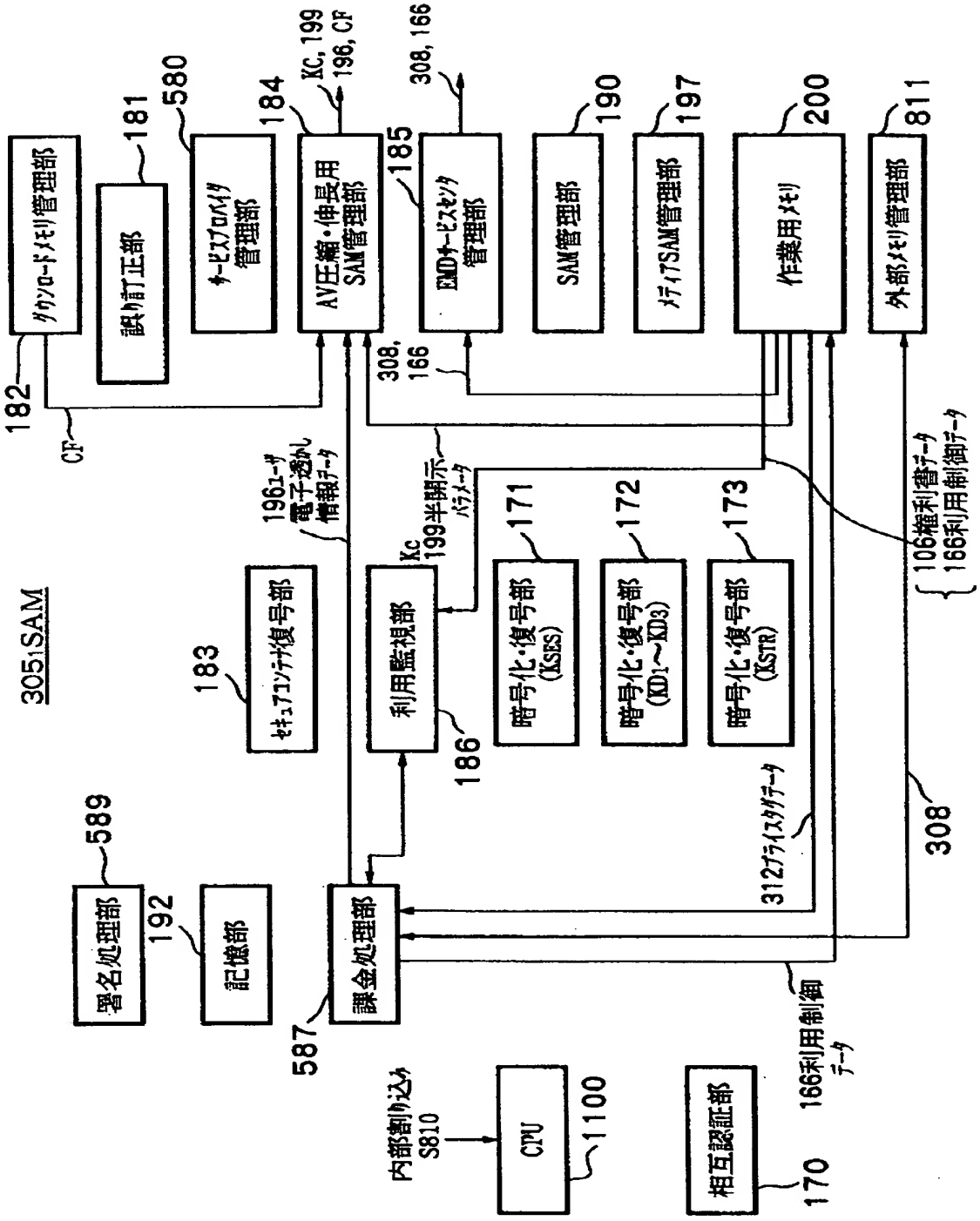

ダウンロードメモリ管理部
182
304
304
304
サービスプロバイダ管理部
580
304
AV圧縮・伸長用SAM管理部
184
EMDサービスセンタ管理部
185
903
KD1～KD3
SIGKD1, ESC
～SIGKD3, ESC
903
SAM管理部
190
メディアSAM管理部
197
作業用メモリ
200
外部メモリ管理部
811
CERCP, CERSP
KF
SAM 1051
利用監視部
186
暗号化・復号部(KSBS)
171
暗号化・復号部(KD1～KD3)
172
暗号化・復号部(KSTR, KMED, KPIN)
173
KD1～KD3
KD1～KD3
KF
署名処理部
589
記憶部
192
課金処理部
587
内部割り込み
S810
CPU
1100
相互認証部
170

【図９１】

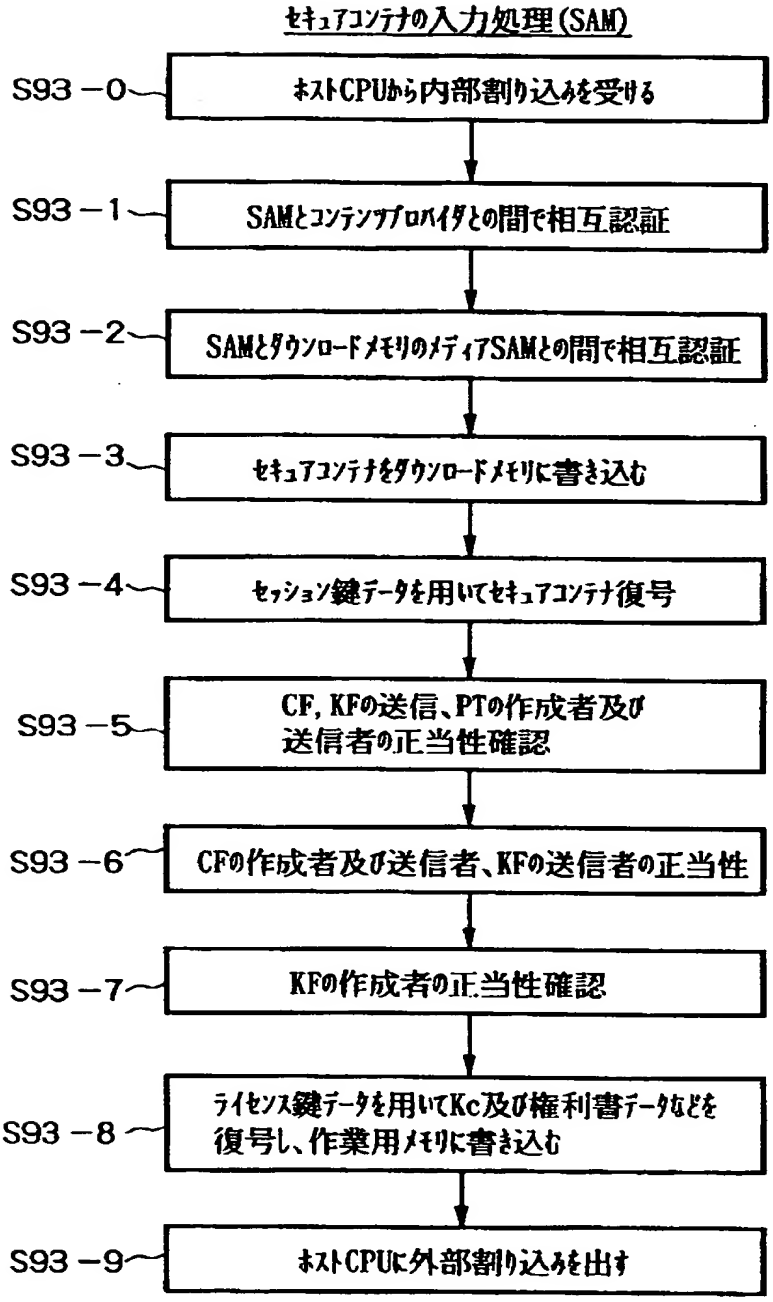
作業用メモリ200の記憶データ

コンテンツ鍵データKc
権利書データ(UCP)106
不揮発性メモリ201のロック鍵データK_{LOC}
コンテンツプロバイダ301の公開鍵証明書データCER_{CP}
サービスプロバイダ301の公開鍵証明書データCER_{SP}
利用制御データ(UCS)166
SAMプログラム・ダウンロード・コンテナSD_1～SDC_3
プライスタグデータ312

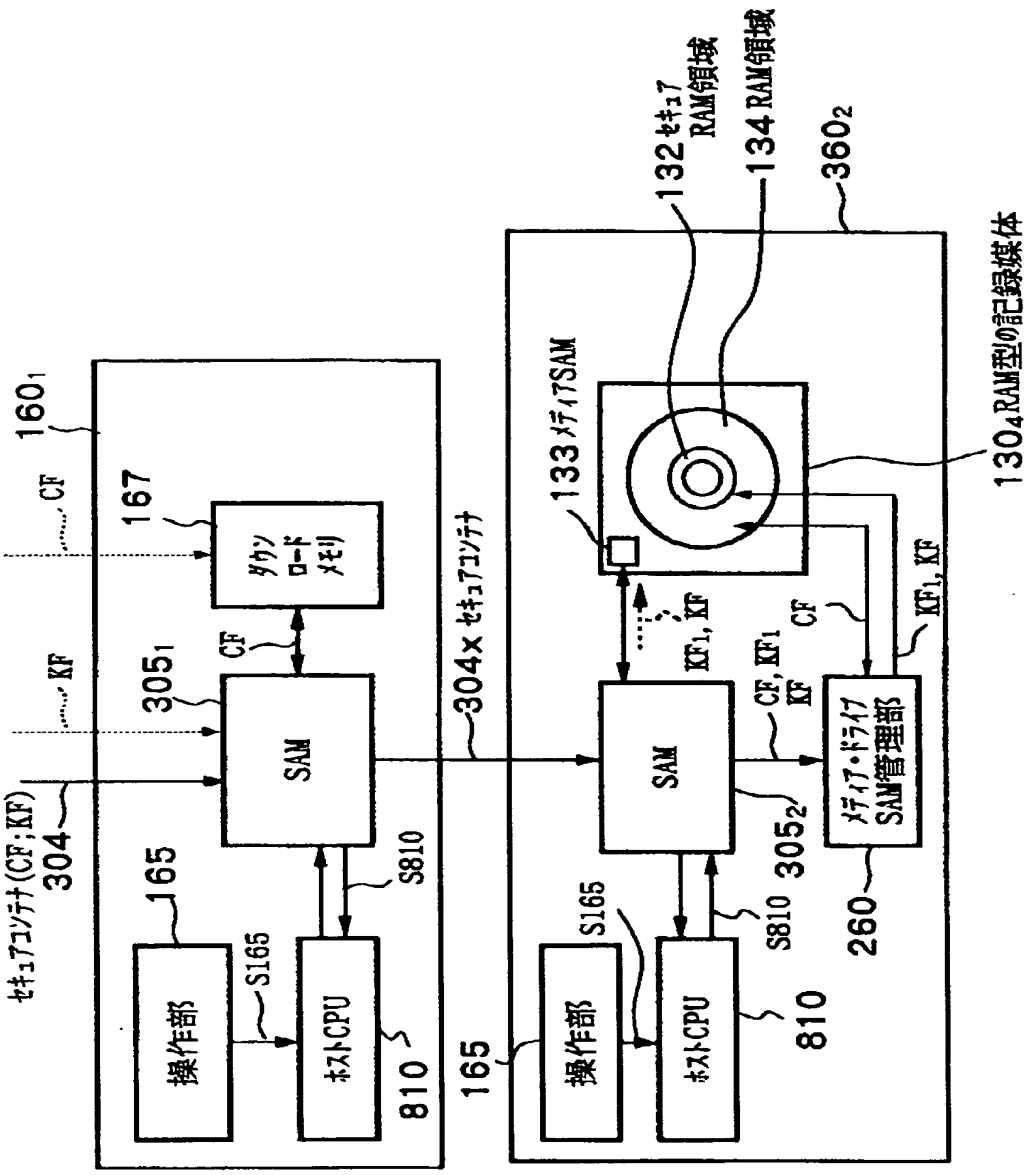
【図９２】


305:SAM
182
CF
ダウンロードメモリ管理部
181
誤り訂正部
580
オーピスプロバイダ管理部
184
KC, 199
196, CF
AV圧縮・伸長用SAM管理部
185
308, 166
EMDオーピスセンタ管理部
190
SAM管理部
197
メディアSAM管理部
200
作業用メモリ
811
外部メモリ管理部
308, 166
196:ユーザ電子透かし情報データ
199半開示パラメータ
Kc
106権利書データ
166利用制御データ
183
セキュアコンテナ復号部
利用監視部
186
171
暗号化・復号部(KSES)
172
暗号化・復号部(KD1～KD3)
173
暗号化・復号部(KSTR)
312ライセンスゲデータ
308
589
署名処理部
192
記憶部
課金処理部
587
内部割り込みS810
CPU
1100
相互認証部
170
166利用制御データ

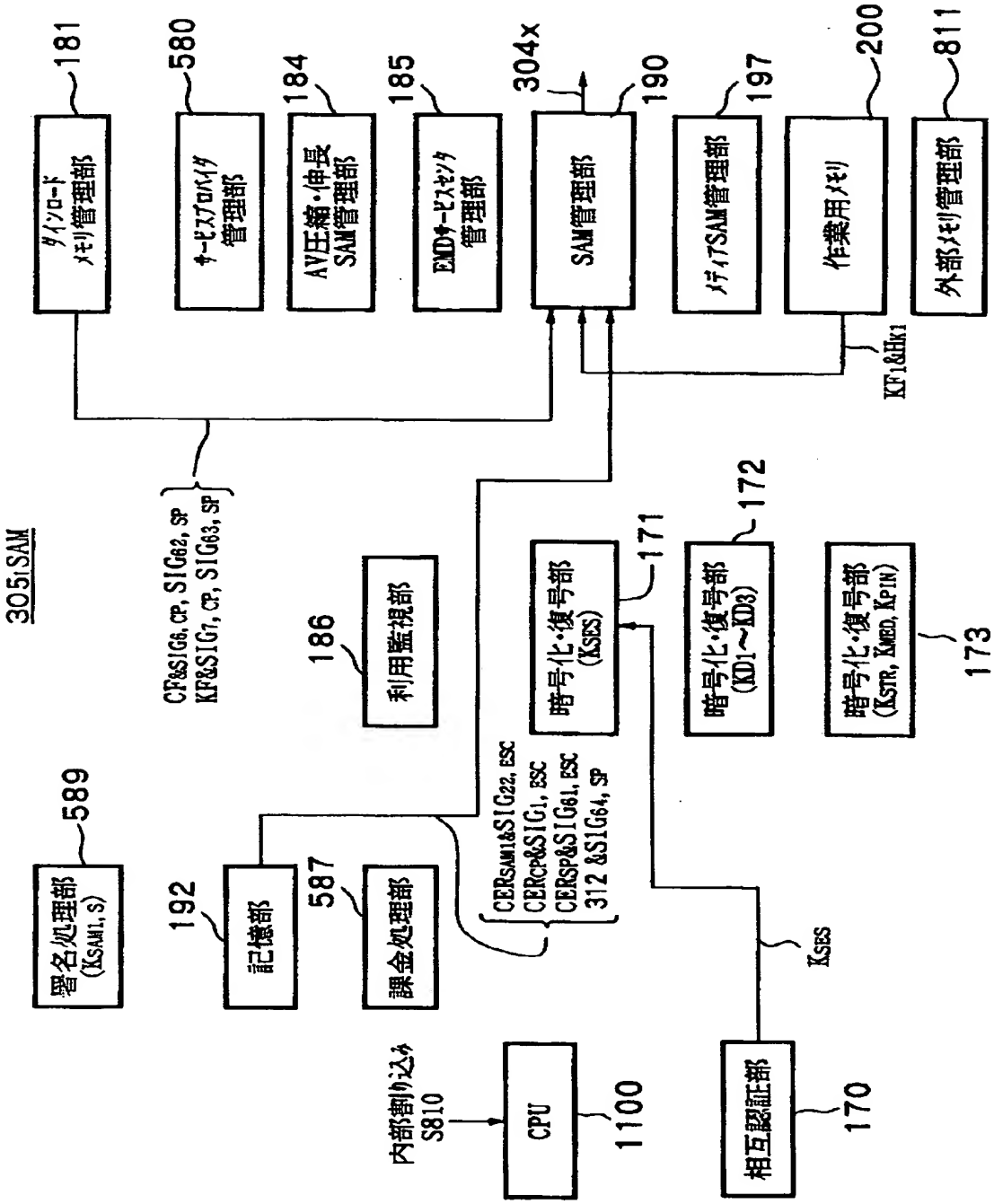
【図９３】


セキュアコンテナの入力処理(SAM)
S93－0
ホストCPUから内部割り込みを受ける
S93－1
SAMとコンテンツプロバイダとの間で相互認証
S93－2
SAMとダウンロードメモリのメディアSAMとの間で相互認証
S93－3
セキュアコンテナをダウンロードメモリに書き込む
S93－4
セッション鍵データを用いてセキュアコンテナ復号
S93－5
CF, KFの送信、PTの作成者及び送信者の正当性確認
S93－6
CFの作成者及び送信者、KFの送信者の正当性
S93－7
KFの作成者の正当性確認
S93－8
ライセンス鍵データを用いてKc及び権利書データなどを復号し、作業用メモリに書き込む
S93－9
ホストCPUに外部割り込みを出す

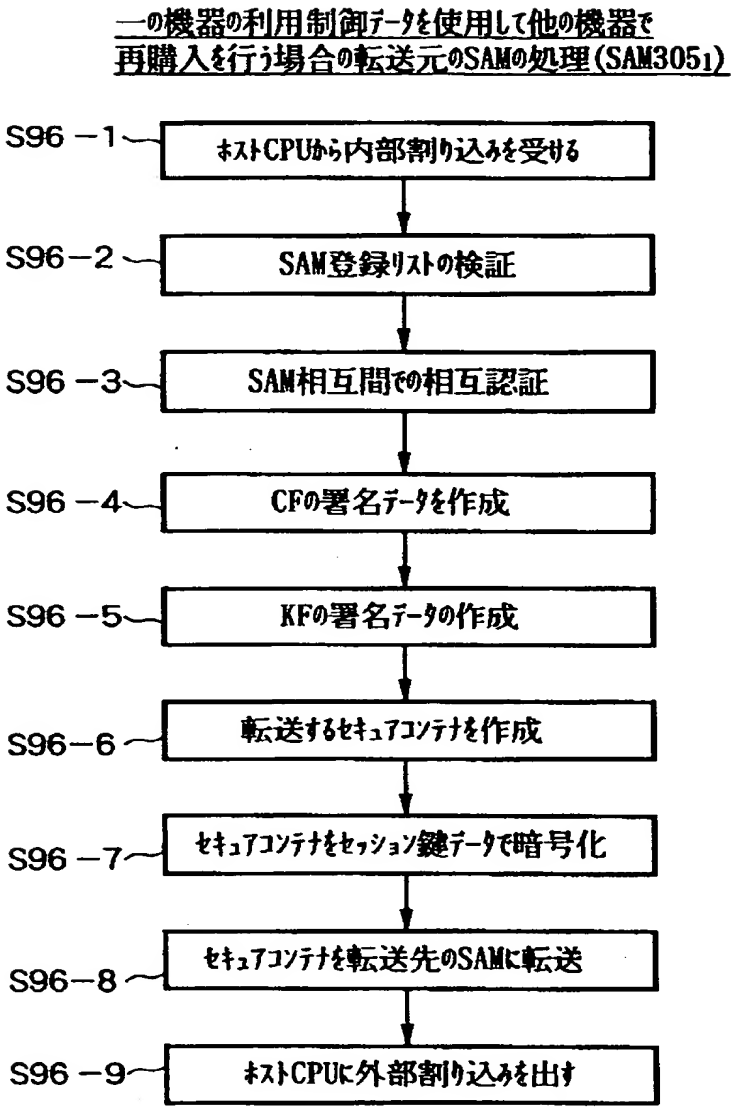
【図９４】


セキュアコンテナ(CF;KF)
304
CF
KF
160₁
167
ダウンロードメモリ
305₁
SAM
165
操作部
S165
ホストCPU
S810
810
304x セキュアコンテナ
133 メディアSAM
132 セキュア RAM領域
134 RAM領域
360₂
130₄ RAM型の記録媒体
KF₁, KF
CF, KF₁
KF
305₂
メディア・ドライブ SAM管理部
260

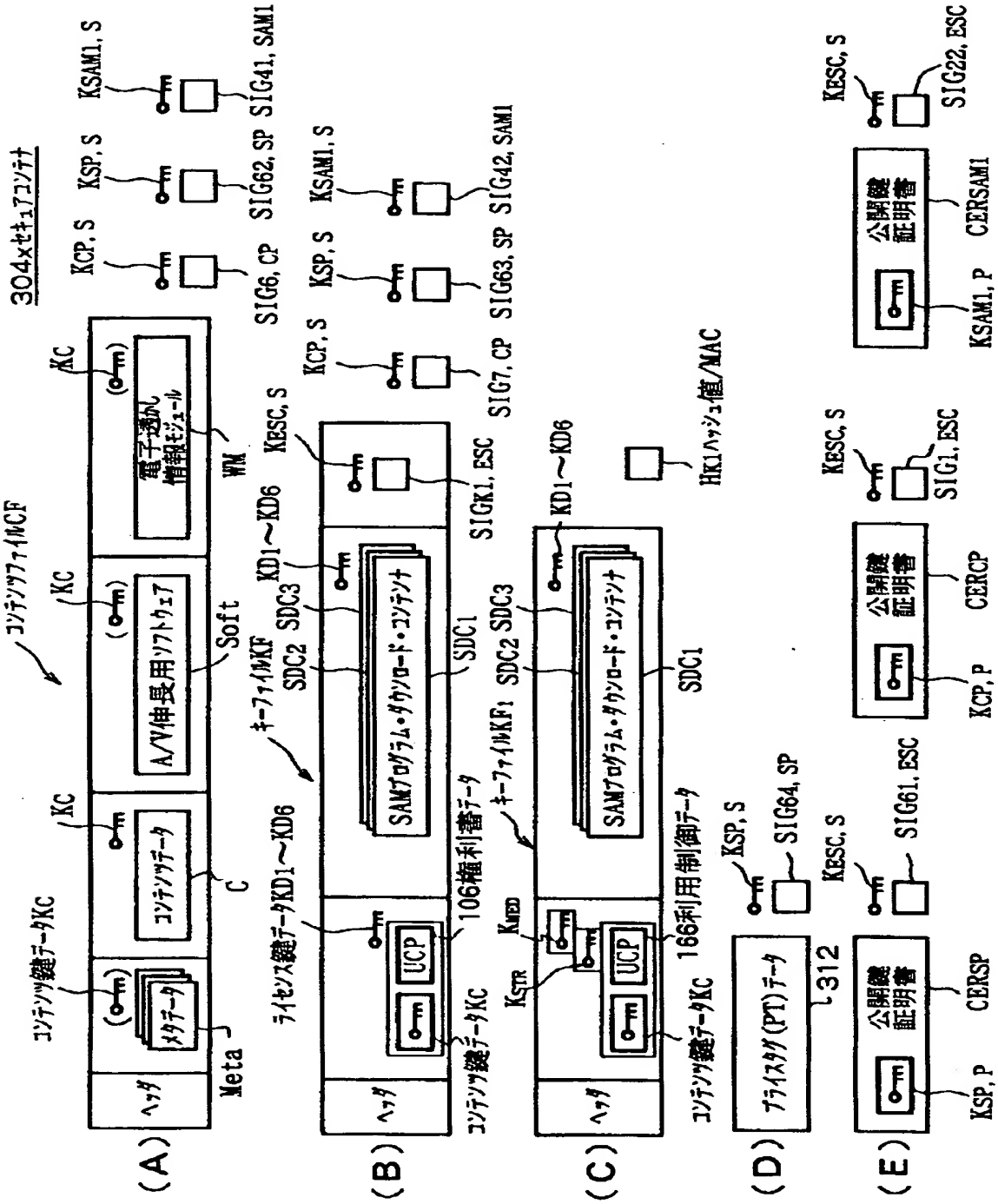
【図９５】


305iSAM
181
ダイソロード メモリ管理部
580
サービスプロバイダ 管理部
184
AV圧縮・伸長 SAM管理部
185
EMDサービスセンタ 管理部
304x
SAM管理部
190
メディアSAM管理部
197
作業用メモリ
200
外部メモリ管理部
811
KF1&HK1
CF&SIG6, CP, SIG62, SP
KF&SIG7, CP, SIG63, SP
186
利用監視部
暗号化・復号部 (KSES)
171
暗号化・復号部 (KD1～KD3)
172
暗号化・復号部 (KSTR, KMED, KPIN)
173
CERSAM1&SIG22, ESC
CERCP&SIG1, ESC
CERSP&SIG61, ESC
312 &SIG64, SP
KSES
署名処理部 (KSAM1, S)
589
192
記憶部
587
課金処理部
内部割り込み S810
CPU
1100
相互認証部
170

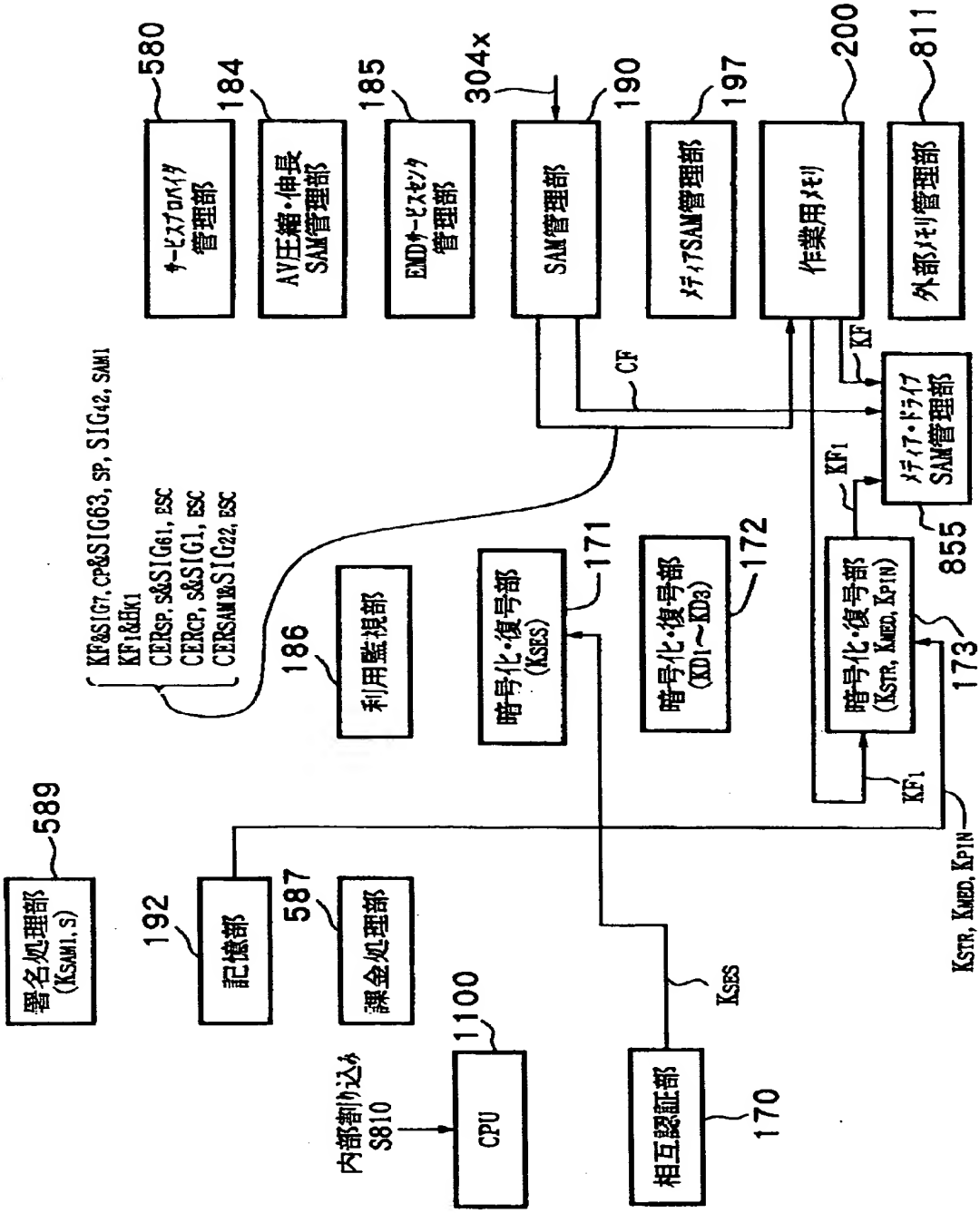
【図９６】


一の機器の利用制御データを使用して他の機器で
再購入を行う場合の転送元のSAMの処理(SAM305₁)
S96－1
ホストCPUから内部割り込みを受ける
S96－2
SAM登録リストの検証
S96－3
SAM相互間での相互認証
S96－4
CFの署名データを作成
S96－5
KFの署名データの作成
S96－6
転送するセキュアコンテナを作成
S96－7
セキュアコンテナをセッション鍵データで暗号化
S96－8
セキュアコンテナを転送先のSAMに転送
S96－9
ホストCPUに外部割り込みを出す

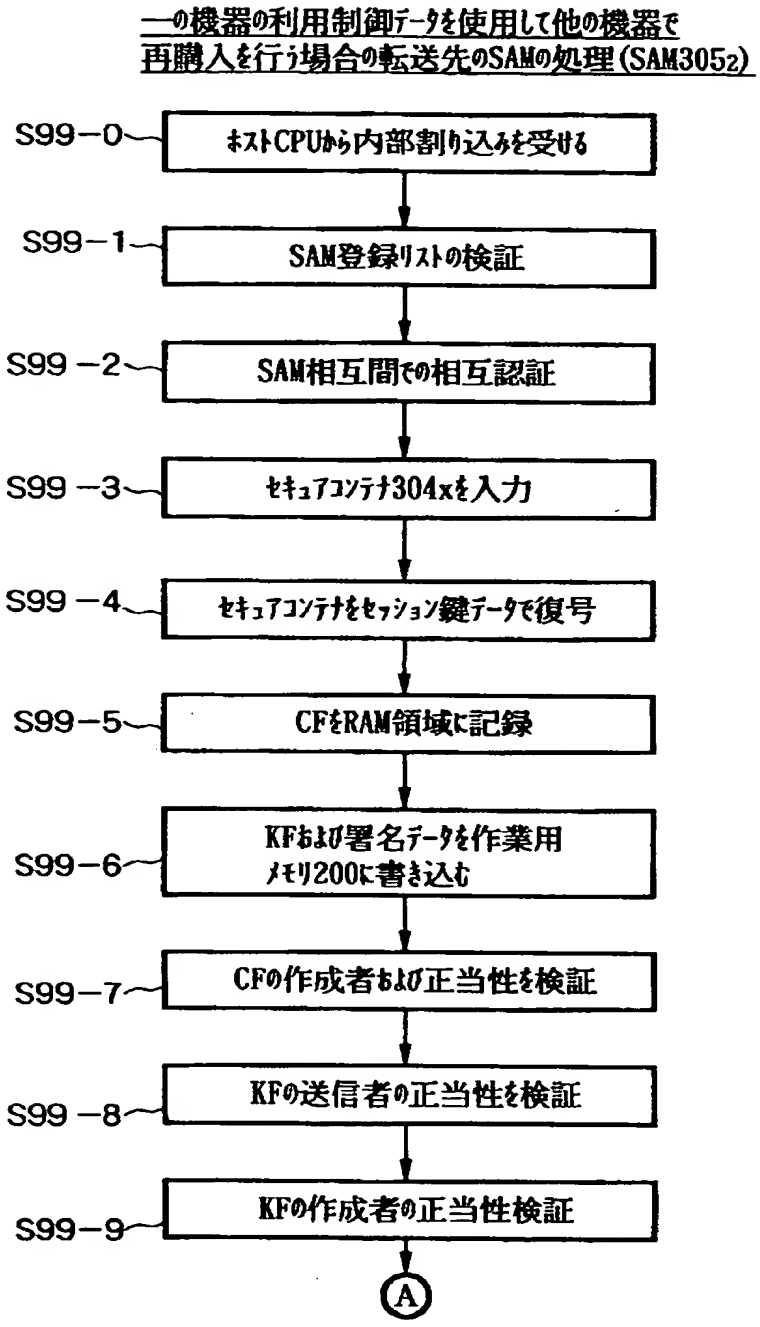
【図９７】


304xセキュアコンテナ
コンテンツファイルCF
(A)
(B)
(C)
(D)
(E)
ヘッダ
メタデータ
Meta
コンテンツデータ
C
A/V伸長用ソフトウェア
Soft
電子透かし情報モジュール
WM
KC
KCP, S
KSP, S
KSAM1, S
SIG6, CP
SIG62, SP
SIG41, SAM1
コンテンツ鍵データKC
ライセンス鍵データKD1～KD6
キーファイルKF
SDC2
SDC3
KD1～KD6
SAMプログラム・ダウンロード・コンテンツ
SDC1
KESC, S
SIGK1, ESC
SIG7, CP
SIG63, SP
SIG42, SAM1
106権利書データ
UCP
KSTR
KMED
キーファイルKF1
166利用制御データ
HK1ハッシュ値/MAC
プライスタグ(PT)データ
312
KSP, S
SIG64, SP
KESC, S
SIG61, ESC
公開鍵証明書
KSP, P
CERSP
KCP, P
CERCP
SIG1, ESC
KSAM1, P
CERSAM1
SIG22, ESC

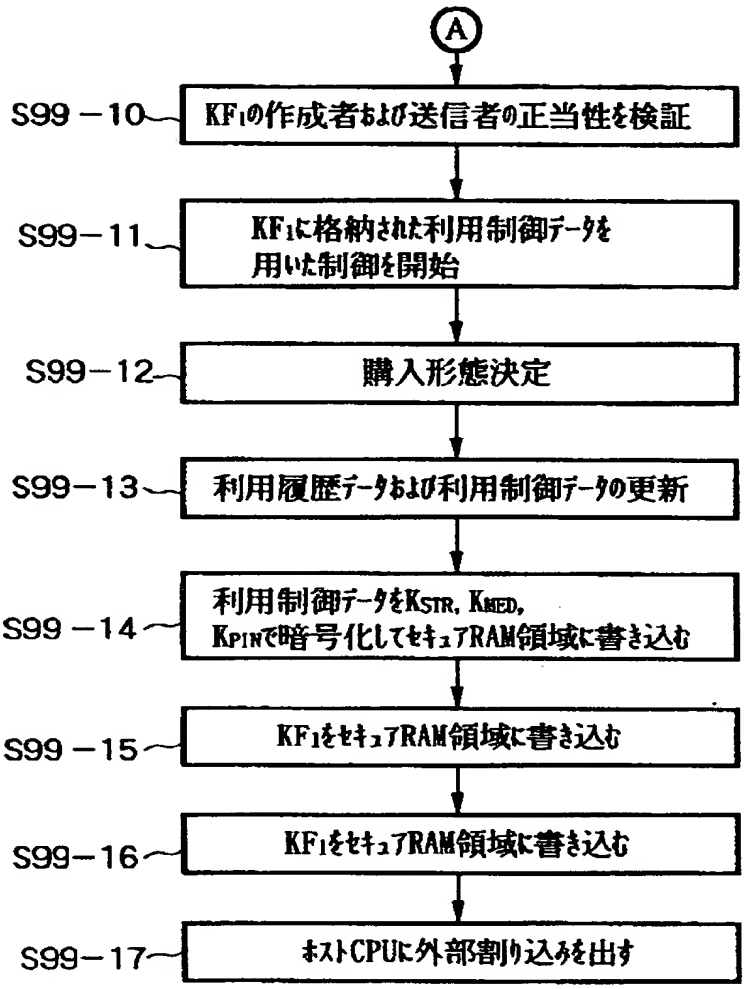
【図９８】


SAM 305₂
580
サービスプロバイダ管理部
184
AV圧縮・伸長SAM管理部
185
EMDサービスセンタ管理部
304x
SAM管理部
190
メディアSAM管理部
197
作業用メモリ
200
外部メモリ管理部
811
CF
KF
メディア・ドライブSAM管理部
855
KF1
KF&SIG7, CP&SIG63, SP, SIG42, SAM1 KF1&EK1
CERSP, S&SIG61, ESC
CERCP, S&SIG1, ESC
CERSAM1&SIG22, ESC
186
利用監視部
暗号化・復号部 (KSES)
171
暗号化・復号部 (KD1～KD3)
172
暗号化・復号部 (KSTR, KMED, KP1N)
173
KF1
KSTR, KMED, KP1N
署名処理部 (KSAM1, S)
589
192
記憶部
587
課金処理部
KSES
1100
CPU
内部割り込み S810
相互認証部
170

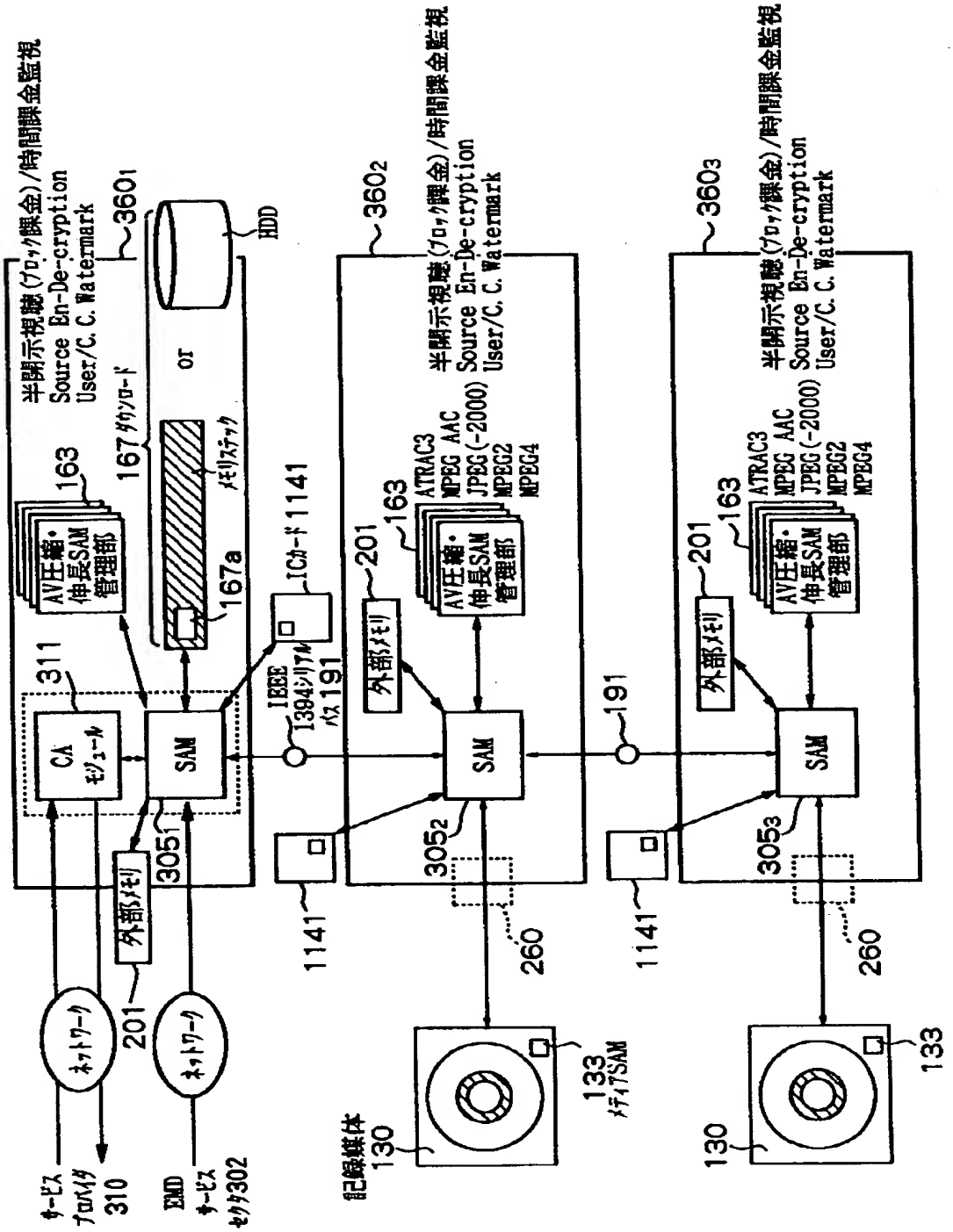
【図９９】


一の機器の利用制御データを使用して他の機器で
再購入を行う場合の転送先のSAMの処理(SAM305₂)
S99-0
ホストCPUから内部割り込みを受ける
S99-1
SAM登録リストの検証
S99-2
SAM相互間での相互認証
S99-3
セキュアコンテナ304xを入力
S99-4
セキュアコンテナをセッション鍵データで復号
S99-5
CFをRAM領域に記録
S99-6
KFおよび署名データを作業用
メモリ200に書き込む
S99-7
CFの作成者および正当性を検証
S99-8
KFの送信者の正当性を検証
S99-9
KFの作成者の正当性検証
A

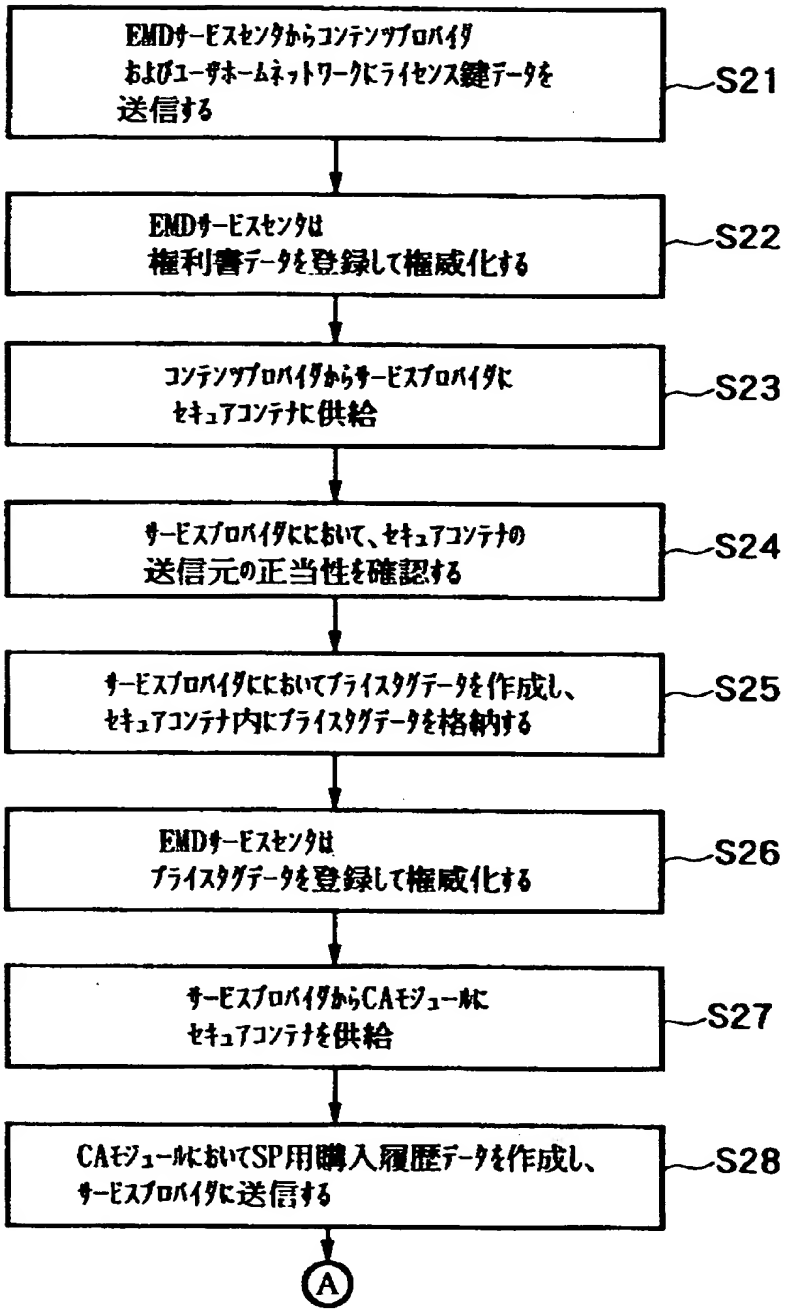
【図１００】


A
S99－10
KF1の作成者および送信者の正当性を検証
S99－11
KF1に格納された利用制御データを用いた制御を開始
S99－12
購入形態決定
S99－13
利用履歴データおよび利用制御データの更新
S99－14
利用制御データをKSTR, KMED, KPINで暗号化してセキュアRAM領域に書き込む
S99－15
KF1をセキュアRAM領域に書き込む
S99－16
KF1をセキュアRAM領域に書き込む
S99－17
ホストCPUに外部割り込みを出す

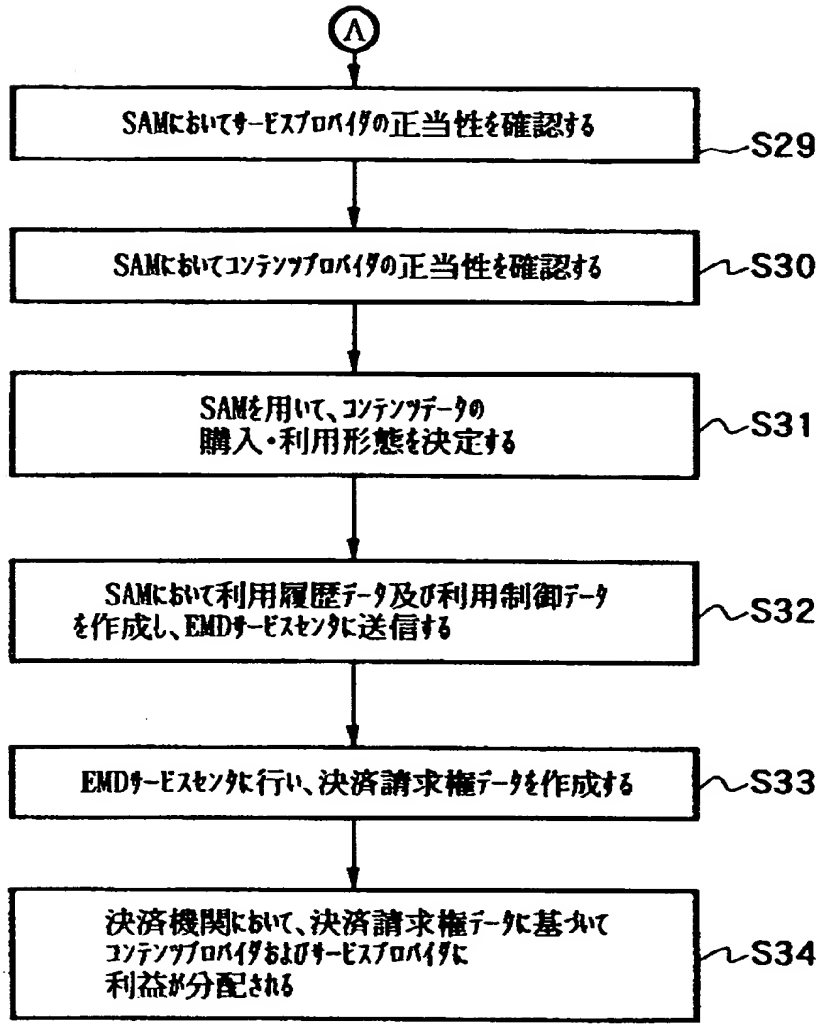
【図１０１】


303
半開示視聴(ブロック課金)/時間課金監視
Source En-De-cryption
User/C. C. Watermark
3601
HDD
or
167 ダウンロード
メモリスティック
163
AV圧縮・伸長SAM管理部
167a
311
CA モジュール
SAM
3051
外部メモリ
201
ICカード1141
IEEE 1394シリアルバス191
ネットワーク
サービスプロバイダ 310
EMD サービスセンタ302
3602
3603
ATRAC3
MPEG AAC
JPEG(-2000)
MPEG2
MPEG4
3052
3053
1141
191
260
133
メディアSAM
記録媒体 130

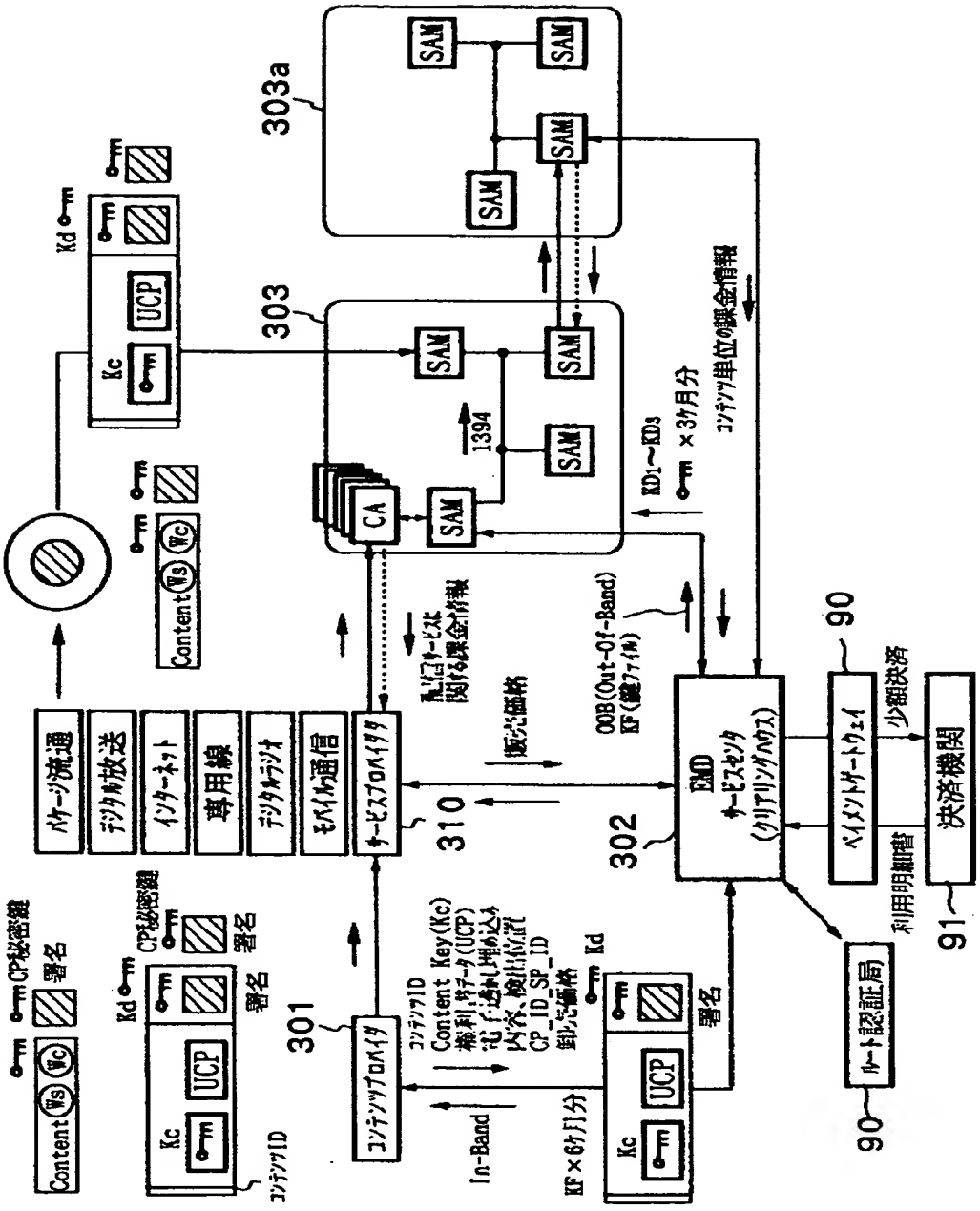
【図１０２】


EMDサービスセンタからコンテンツプロバイダ
およびユーザホームネットワークにライセンス鍵データを
送信する
S21
EMDサービスセンタは
権利書データを登録して権威化する
S22
コンテンツプロバイダからサービスプロバイダに
セキュアコンテナに供給
S23
サービスプロバイダにおいて、セキュアコンテナの
送信元の正当性を確認する
S24
サービスプロバイダにおいてプライスタグデータを作成し、
セキュアコンテナ内にプライスタグデータを格納する
S25
EMDサービスセンタは
プライスタグデータを登録して権威化する
S26
サービスプロバイダからCAモジュールに
セキュアコンテナを供給
S27
CAモジュールにおいてSP用購入履歴データを作成し、
サービスプロバイダに送信する
S28
A

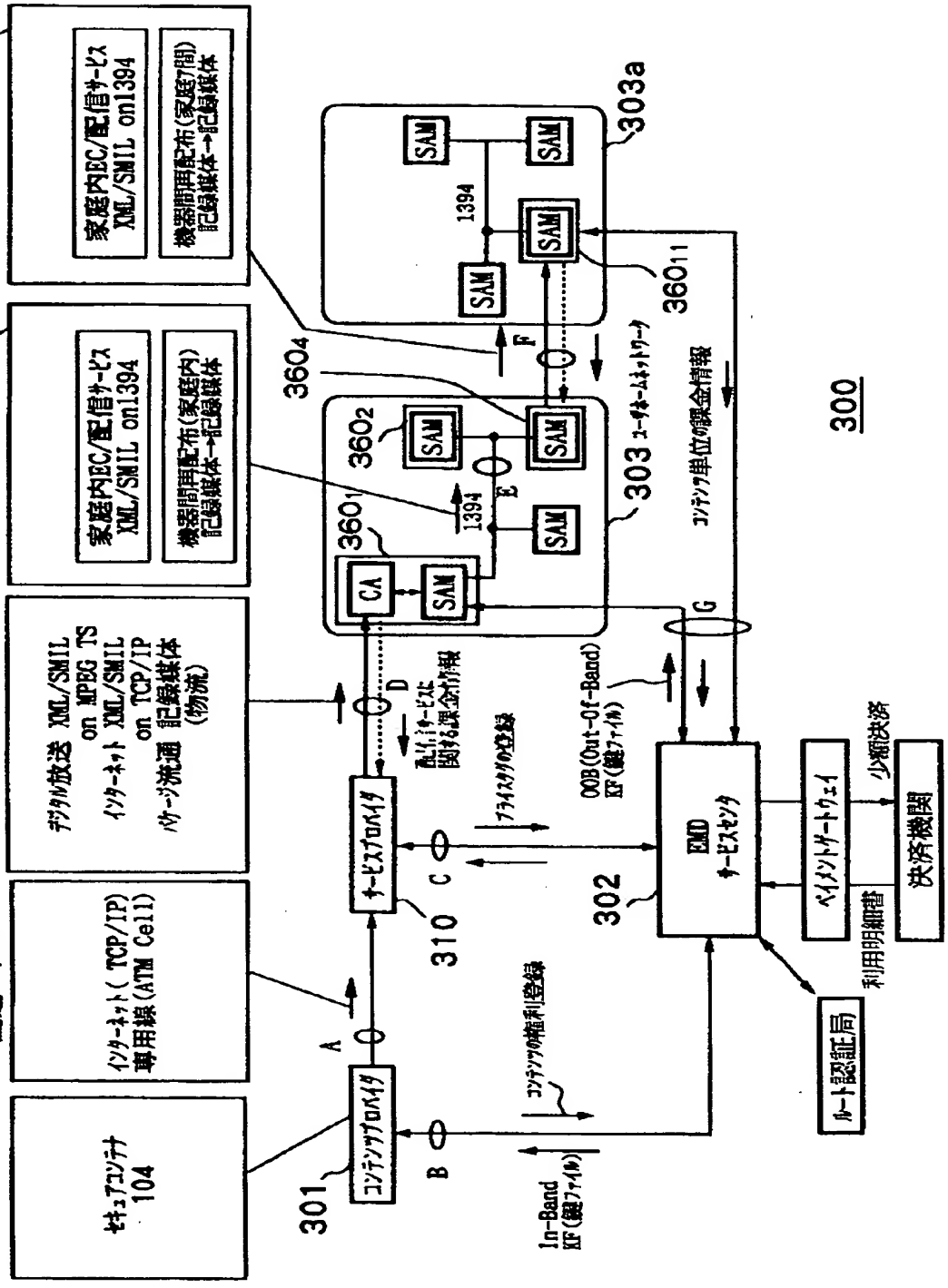
【図１０３】


A
SAMにおいてサービスプロバイダの正当性を確認する
S29
SAMにおいてコンテンツプロバイダの正当性を確認する
S30
SAMを用いて、コンテンツデータの
購入・利用形態を決定する
S31
SAMにおいて利用履歴データ及び利用制御データ
を作成し、EMDサービスセンタに送信する
S32
EMDサービスセンタに行い、決済請求権データを作成する
S33
決済機関において、決済請求権データに基づいて
コンテンツプロバイダおよびサービスプロバイダに
利益が分配される
S34

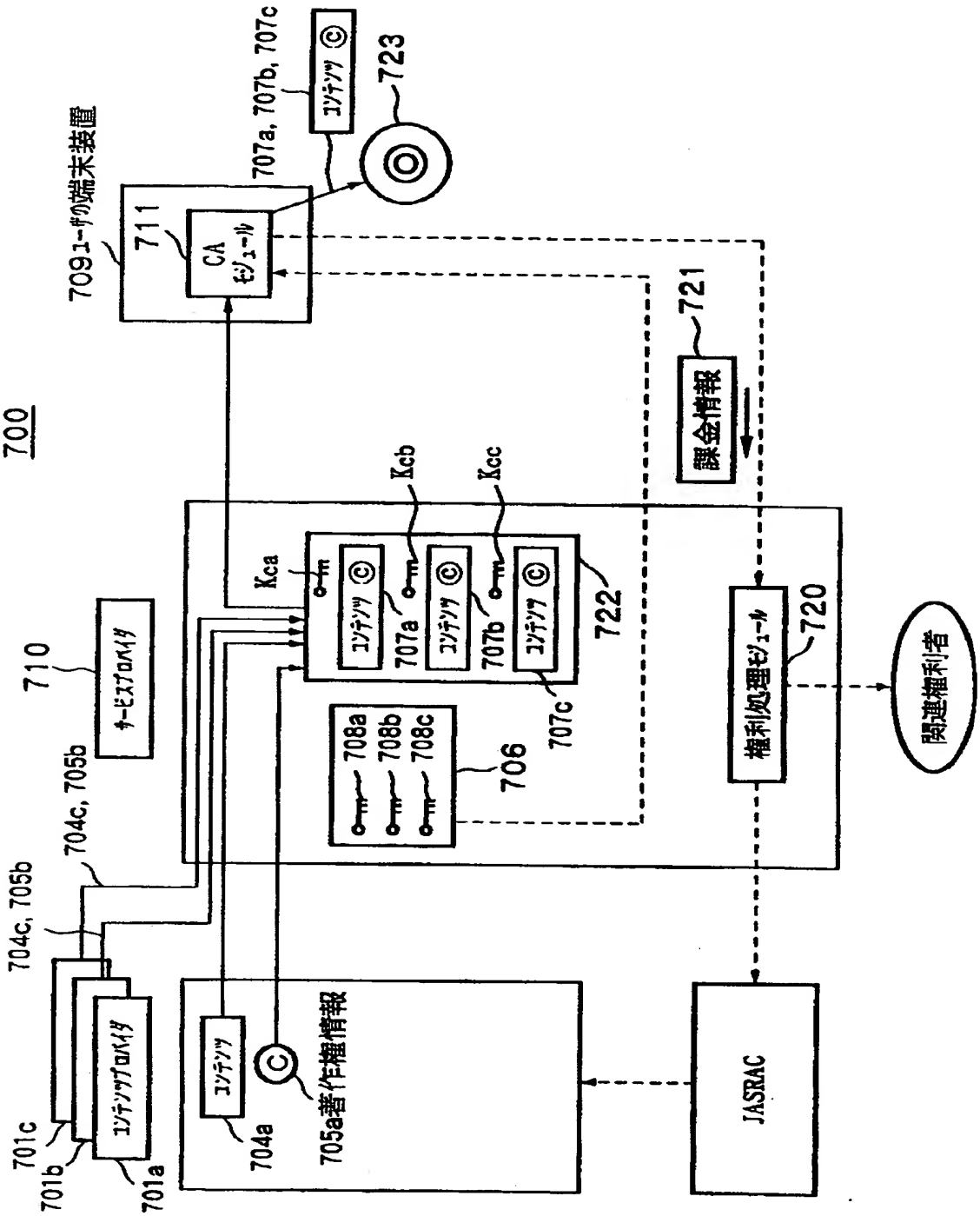
【図１０４】


303a
SAM
303
CA
1394
Kd
Kc
UCP
Content
Wc
Ws
CP秘密鍵
署名
コンテンツID
パケット流通
デジタル放送
インターネット
専用線
デジタルラジオ
モバイル通信
サービスプロバイダ
310
301
コンテンツプロバイダ
In-Band
Content Key(Kc)
権利情報データ(UCP)
CP_ID_SP_ID
KF×6ヶ月分
KD1～KD3
×3ヶ月分
コンテンツ単位の課金情報
販売価格
OOB(Out-Of-Band)
KF(鍵ファイル)
EMD
サービスセンタ
(クリアリングハウス)
302
ペイメントゲートウェイ
少額決済
決済機関
91
90
利用明細書
ルート認証局

【図１０５】


家庭間EC/機器間
再配布用の再送プロトコル
家庭内EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭間)
記録媒体→記録媒体
家庭内EC/機器間
再配布用の再送プロトコル
家庭内EC/配信サービス
XML/SMIL on1394
機器間再配布(家庭内)
記録媒体→記録媒体
サービスプロバイダ用
配送プロトコル
デジタル放送 XML/SMIL
on MPEG TS
インターネット XML/SMIL
on TCP/IP
パッケージ流通 記録媒体
(物流)
コンテンツプロバイダ用
配送プロトコル
インターネット(TCP/IP)
専用線(ATM Cell)
セキュアコンテナ
104
301
コンテンツプロバイダ
310
サービスプロバイダ
302
EMD
サービスセンタ
303
ユーザホームネットワーク
303a
SAM
CA
1394
360₁
360₂
360₃
360₄
360₁₁
A
B
C
D
E
F
G
In-Band
KF(鍵ファイル)
コンテンツの権利登録
配信サービスに
関する課金情報
プライスタグの登録
OOB(Out-Of-Band)
KF(鍵ファイル)
コンテンツ単位の課金情報
ペイメントゲートウェイ
決済機関
少額決済
利用明細書
ルート認証局
300

【図１０６】


700
709ユーザの端末装置
711
CA モジュール
707a, 707b, 707c
コンテンツ
723
721
課金情報
710
サービスプロバイダ
Kca
Kcb
Kcc
722
707a
707b
707c
708a
708b
708c
706
720
権利処理モジュール
関連権利者
704c, 705b
704c, 705b
701c
701b
701a
コンテンツプロバイダ
704a
コンテンツ
705a著作権情報
JASRAC

【書類名】　要約書

【要約】

【課題】　コンテンツデータの提供者の利益を効果的に保護できるデータ処理装置を提供する。

【解決手段】　ＳＡＭ１０５$_1$は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す権利書データとを格納したセキュアコンテナ１０４を入力し、権利書データが示す取り扱いに基づいて、コンテンツデータの購入形態および利用形態の少なくとも一方を決定する。ＳＡＭ１０５$_1$は、ホストＣＰＵ８１０のスレーブとして機能すると共に、ホストＣＰＵ８１０との共有メモリを有している。

【選択図】　図２２

出 願 人 履 歴 情 報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社